NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MICROSOFT WINDOWS SERVER 2003: SECURITY ENHANCEMENTS AND NEW FEATURES

by

Ronald Centeno Montehermoso

September 2004

Thesis Advisor:	Douglas E. Brinkley
Second Reader:	Glenn R. Cook

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Microsoft Windows Server 2003: Security Enhancements and New Features			**5. FUNDING NUMBERS**
6. AUTHOR(S) Ronald Montehermoso			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The purpose of this thesis is to discuss the new features and enhancements of Windows Server 2003. Windows NT and Windows 2000 were known to have numerous security vulnerabilities; hence Microsoft focused on improving security by making Windows Server 2003 "secure by design, secure by default, secure in deployment." This thesis examines the differences between the five unique editions of the Windows Server 2003 family. Some of the pros and cons of migrating to Windows Server 2003 are highlighted. The author hopes this study will assist information technology professionals with their decision on whether or not to upgrade to this latest version of Microsoft's flagship network operating system.

14. SUBJECT TERMS Information Systems, Information Technology, Information Technology Management, Local Area Networks, Wide Area Networks, Network Operating Systems, Microsoft Windows Server 2003			**15. NUMBER OF PAGES** 137
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

MICROSOFT WINDOWS SERVER 2003: SECURITY ENHANCEMENTS AND NEW FEATURES

Ronald C. Montehermoso
Lieutenant Commander, United States Navy
B.S./B.A., University of San Diego, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2004

Author: Ronald Centeno Montehermoso

Approved by: Douglas E. Brinkley
Thesis Advisor

Glenn R. Cook
Second Reader

Daniel C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this thesis is to discuss the new features and enhancements of Windows Server 2003. Windows NT and Windows 2000 were known to have numerous security vulnerabilities; hence Microsoft focused on improving security by making Windows Server 2003 "secure by design, secure by default, secure in deployment." This thesis examines the differences between the five unique editions of the Windows Server 2003 family. Some of the pros and cons of migrating to Windows Server 2003 are highlighted. The author hopes this study will assist information technology professionals with their decision on whether or not to upgrade to this latest version of Microsoft's flagship network operating system.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First, I would like to thank God for giving me this opportunity for higher education, guiding me to overcome challenges at school and at home. Especially, He has continued to provide me with strength when I am reminded daily of my eldest brother, Manual Centeno Montehermoso, who recently passed away on July 02, 2003, and was to attend the Naval Postgraduate School in January 2004. I will always remember my brother and his superb achievements in high school and in college. I can only aspire to be as smart as him.

Again, I would like to thank God for a loving family. I have been truly blessed by and am very appreciative of all the support and love given to me by my wife, Renelynne Porciuncula Montehermoso. Without her I would not be here today. She has been my light, guiding me through this arduous journey. Of course, I give thanks to my loving children, Ronald Matthew and Jocelynne Marie, for keeping the kid in me alive and jovial.

Lastly, it was my pleasure and honor to have worked with two of the best educators staffed at the Naval Postgraduate School. My thesis advisor Doug Brinkley and my thesis second reader Glenn Cook. Thank you for the guidance. God bless.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Microsoft Windows is one of the most commonly used operating systems worldwide, whether in the home or in the office. Currently with about 43 percent of servers running a Microsoft Windows product, Microsoft has the largest market share in operating systems [Ref. 1]. In its most recent version, Microsoft Windows Server 2003, Microsoft has strived to deliver an operating system with unparalleled security features. This thesis examines the security improvements that make Windows Server 2003 more "secure by design, secure by default, and secure in deployment" than its predecessors [Ref. 2].

When Microsoft released Windows Server 2003 in April 2003, the executives of Microsoft expected the operating system to meet the challenges of their Trustworthy Computing Initiative presented on January 15, 2002 by Chairman and Chief Software Architect Bill Gates [Ref. 3]. This thesis will explore how those challenges were met by examining the new security features introduced in the operating system and examine the differences between the various editions of the Windows Server 2003 family.

A. BACKGROUND

On January 15, 2002, Microsoft Chairman and Chief Software Architect Bill Gates delivered a company-wide memo that outlined his concept called "trustworthy computing." He challenged his company to improve the experiences of Microsoft customers in regards to a concept that Microsoft has come to call the "four pillars" of trustworthy computing. The Trustworthy Computing Initiative consists of the four pillars known as security, privacy, reliability, and business integrity. Security provides customers a system that is resilient to attack, and ensures confidentiality, integrity, and availability of the system and protection of its data. Privacy gives users the ability to control data about themselves and assures whoever uses their data does so in a faithful manner and adheres to fair information principles. Reliability ensures Windows Server 2003 can be depended on to fulfill its function. Lastly, having business integrity allows vendor products to behave in a responsive and responsible manner. In developing their software, Microsoft focused on the four pillars, soliciting their customers' recommendations on how Microsoft could best deliver a more secure and trustworthy

computing experience. Microsoft executives traveled around the world and literally talked to thousands of customers to get their valued input. [Ref. 3]

From its customers, Microsoft gained a lot of valuable insight that made the software giant revamp its operating system to meet its goal of a more trustworthy computing environment. Microsoft's Windows division spent nearly $100 million to provide greater security in four areas: design, default, deployment, and customer communications [Ref. 3]. Microsoft executives state these areas will continue to be Microsoft's focus in its current Windows Server family and up to the new generation that is scheduled to be released in 2006.

Network World Fusion selected Microsoft's Server 2003 as the top network operating system after testing major operating systems designed to run on enterprise-level servers [Ref. 4]. The other operating systems evaluated were NetWare 6.5, Red Hat Linux Advanced Server 9.0, SuSe Linux, and Apple's OS/X 10.2.5. Microsoft Server 2003 was considered a flexible and versatile platform in respect to installation and management. The five editions of the Windows Server 2003 family are the following:

- **Windows Server 2003, Standard Edition -** Designed for departmental and standard workloads, and provides a high level of dependability, scalability, and security [Ref. 5].
- **Windows Server 2003, Enterprise Edition -** Primarily supports high-performance servers by clustering servers for greater load handling that increase availability of systems [Ref. 6].
- **Windows Server 2003, Datacenter Edition -** Mainly developed for systems requiring high levels of scalability and reliability in order to support mission-critical solutions for databases, enterprise resource planning software, high-volume and real-time transaction processing, and server consolidation [Ref. 7].
- **Windows Server 2003, Web Edition -** Designed to provide a single-purpose solution for Internet service providers, application developers, and professionals desiring to use or deploy specific Web functionality [Ref. 8].
- **Windows Small Business Server 2003 -** Enables Information Technology (IT) professionals to deploy small businesses' systems that are more secured and reliable [Ref. 9].

The Windows Server 2003 family is founded upon the proven technology of Windows 2000 server and strives to deliver an operating system that is easier to deploy, manage, and use.

B. PURPOSE

The trustworthy computing concept has been marketed by Bill Gates as a means to satisfy Microsoft's customers. This drive has influenced the end product of Windows Server 2003 to become more secure. The intended audience for this thesis is IT professionals who are already familiar with Microsoft Windows operating systems. The objective of this thesis is to introduce Microsoft Windows Server 2003 and the new features of the operating system. The purpose of thesis is to examine the following:

- What security features are introduced in Windows Server 2003?
- Is Windows Server 2003 more secure than previous operating systems?
- What are the differences between the Windows Server 2003 family editions?
- Should the Department of Defense (DoD) migrate to Windows Server 2003?

C. THESIS ORGANIZATION

Windows Server 2003 will be the focus of this thesis and the questions above will be thoroughly expounded on and examined in the chapters. The organization of the thesis is as follows:

- Chapter I -This chapter introduces the topic of interest by highlighting the objectives of this thesis.
- Chapter II - This discusses the Windows Server 2003 security features and improvements.
- Chapter III -This chapter explores the Windows Server 2003 family editions, features, and technologies introduced in the operating system.
- Chapter IV - This addresses significant pros and cons for an organization migrating to Windows Server 2003.
- Chapter V - The research report conclusions are presented in this fnal chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WINDOWS SERVER 2003 SECURITY FEATURES AND IMPROVEMENTS

Windows Server 2003 is the first product from Microsoft to be developed and designed under the Trustworthy Computing Initiative issued by Bill Gates in January 2002. This initiative is the foundation of Windows Server 2003 and its security features and improvements. Some of the new security-related features in Windows Server 2003 include design changes, network security, authentication, access control, public key infrastructure, data encryption, auditing, and the tools offered in the operating system [Ref. 10]. Microsoft's framework for the new operating system has been focused toward security objectives and goals that have produced a server that is "secure by design," "secure by default," and "secure in deployment." The Windows Server 2003 operating systems are as robust as their predecessors, with similar features but with improved security.

Windows Server 2003 has been developed to be "secure by design" in the manner where security is improved by reducing the code vulnerabilities of the platform, by modifying developmental processes, and by improving accountability at every security level. In addition, features in Windows Server 2003 have been redesigned to improve its Internet Information Services, to create stronger authentication protocols such as 802.1X and the Protected Extensible Authentication Protocol (PEAP), and to utilize the common language runtime in order to create a safer computing environment. [Ref. 11]

In regards to "secure by default," it is a goal for Microsoft Corporation and other software vendors "straight from the box" to deliver a product that is more secure by disabling services that are not required by the customer and by limiting the permissions granted automatically to users [Ref. 1]. By making these changes, the administrator of the system will be relied upon to appropriately monitor and manage the services. In addition, strict adherence to policies will affect the network system's ability to maintain a secure environment.

"Secure in deployment" is a vision Microsoft hopes to achieve through continuous support to customers. Essentially, Microsoft has offered its customers tools,

prescriptive guidance, training, and services that have helped in the deployment of a secure infrastructure. Microsoft's key goals are to assist customers in the following distinct areas:

- Protecting systems by ensuring only trusted users have access, and properly configuring and updating as needed in order to assist in keeping unauthorized users out.
- Detecting and alerting any attempts of intrusions, violations of security, operational problems, unexpected behavior, or pre-failure indications into the system.
- Defending systems by automatically taking the corrective action required when a security violation is detected.
- Recovering computers from compromise or failure by depending on the systems and processes in place to restore the computer and its data to its latest known good state, while reducing the downtime required to correct the system.
- Managing and coordinating the means to protect, detect, defend, and recover critical systems. [Ref. 11]

Through Microsoft's technological advances, the Trustworthy Computing Iinitiative is the basis of Windows Server 2003's new security features and improvements that address a secure platform, a deployment of public key infrastructure, and a secure extension of an organization to the Internet. This chapter will further discuss the new security improvements and features in Windows Server 2003 that help explain how an organization's information technology infrastructure can have the capability to create solutions that can meet its business objectives and at the same time protect its information assets.

A. SECURE PLATFORM

Due to the rapid growth in technology and the use of computers, commercial businesses have optimized computers in every day business by expanding traditional local area networks that use intranets, extranets, and Internet sites. This increase in the use of information technological advancements has also spurred the desire for increased security of information systems. In addition, hacker and cyber attacks have increased as well, which is Microsoft's concern in providing a secure platform that will be proven in the Windows Server 2003 family edition. The new operating systems use a combination of new security features and improvements that will provide a more secure platform.

1. Internet Connection Firewall (ICF)

The ICF is a software-based firewall that provides protection to computer systems connected to the Internet and/or to computers located behind the Internet connection sharing a host computer running ICF. In today's society, many home and corporate computer users have their systems always on and connected to the Internet. Unfortunately, this leaves their systems open to attack. By using an ICF, the user can create a barrier by making it difficult for the hacker to get into one's computer.

Essentially, the ICF grants permission to outgoing communications originating from one's computer and at the same time blocks everything else. The ICF can be viewed as a stateful-inspection packet filter. The following is a brief description of how the ICF filters packets during Web surfing:

- URL is entered by the user via the browser.
- Request is sent to the Internet by the user's computer with an address destination of the Web server.
- The traffic is seen leaving the user's computer by the ICF which maintains the specific of the connection.
- Reply is created by the Web server which addresses and sends it back to the user.
- Finally, stateful-inspection packet filter occurs: the incoming traffic is seen and the specific are compare to what was seen before by the ICF. The ICF will allow the reply through if the specifics match.
- The page requested is displayed by the user's browser. [Ref. 12]

The above process is very simple, and unfortunately protecting a computer is not as simple. A single firewall or any protective measure by itself will not be sufficient enough to secure a computer system. Systems administrators must diligently install a firewall, install anti-virus software and frequently update it, and ensure computer systems are up-to-date in regards to security patches.

2. Secure Internet Authentication Server (IAS) and Remote Authentication Dial-In User Server (RADIUS)

RADIUS, an industry standard for client server protocol, uses IAS to have the capability to manage user authentication, authorization, auditing, and accounting of network connection attempts. In addition, IAS can manage connections to the network using various connectivity technologies, such as dial-up, virtual private networks, and

firewalls. Basically, IAS is the implementation of the RADIUS server that consolidates authentication and authorization in order to centrally manage all access servers, as well as auditing and accounting tasks, through a single set of rules that is applied throughout the wired, wireless, virtual private network (VPN), and dial-up access. Also, IAS can be implemented in a RADIUS proxy that allows the routing of RADIUS messages between RADIUS clients, proxies, servers that performing authentication, authorization, auditing, and accounting of connection attempts to the network. [Ref. 13]

In Figure 1, IAS/RADIUS infrastructure has five components: access clients, access servers (RADIUS clients), IAS servers (RADIUS servers), IAS proxies (RADIUS proxies), and user account databases.

- Access clients are devices requiring some level of access to a larger network, such as dial-up or VPN clients, wireless clients, or LAN clients connected to an authenticating switch.
- Access servers used as RADIUS clients are devices that provide some level of access to a larger network, and sends connection requests and accounting messages to a RADIUS server.
- IAS servers used as RADIUS servers are devices that receive and process connection requests or accounting messages sent by RADIUS clients or RADIUS proxies. For connection requests, the RADIUS server authenticates and authorizes the connection by processing a list of RADIUS attributes based on a set of rules and the information in the user account database. After processing, the RADIUS server sends back either an Access-Accept message, containing connection restrictions implemented by the access server, or an Access-Reject message.
- IAS proxies and RADIUS proxies are devices that forward or route RADIUS connection requests and accounting messages. The information within the RADIUS message is used by the RADIUS proxy to route the message to the appropriate RADIUS server.
- User Account Databases list the user accounts and their properties checked by a RADIUS server that verifies the authentication credentials and the user account properties containing the authorization and connection parameter information. IAS can use the local Security Accounts Manager (SAM). But, if the user accounts for authentication reside in different types of databases, such as in an Active Directory that may include untrusted forests, untrusted domains, or one-way trusted domains, IAS can be configured as a RADIUS proxy to forward the authentication request. [Ref. 13]

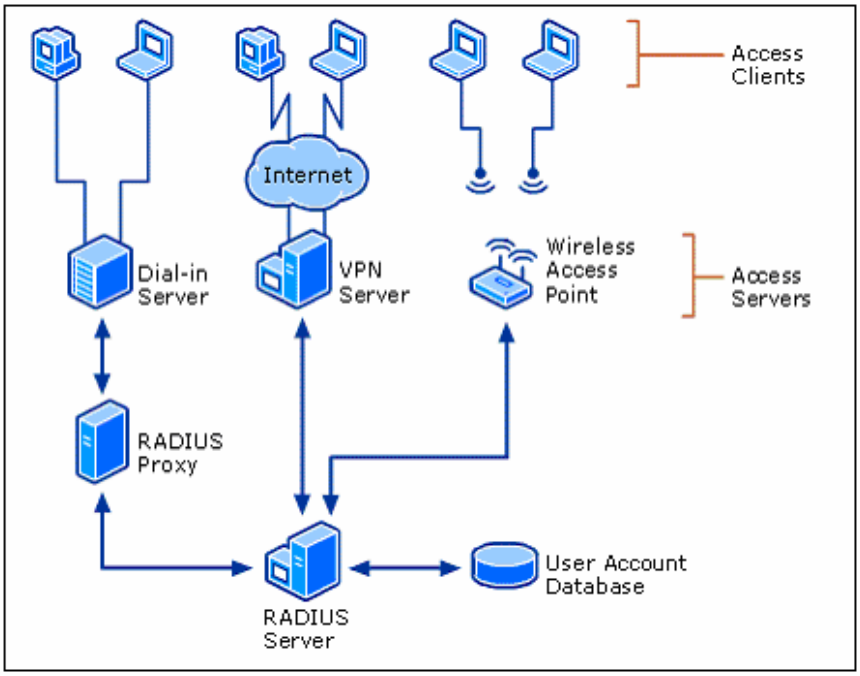

Figure 1. Components of an IAS/RADIUS Infrastructure. (From Ref. [13].)

Another aspect of IAS/RADIUS is depicted in Figure 2, which shows a single infrastructure and a single network that have a centrally managed infrastructure using IAS and RADIUS. This security-enhanced and centrally managed network can support network access for wireless, VPN, wired, and dial-up by tightly integrating authentication and security services.

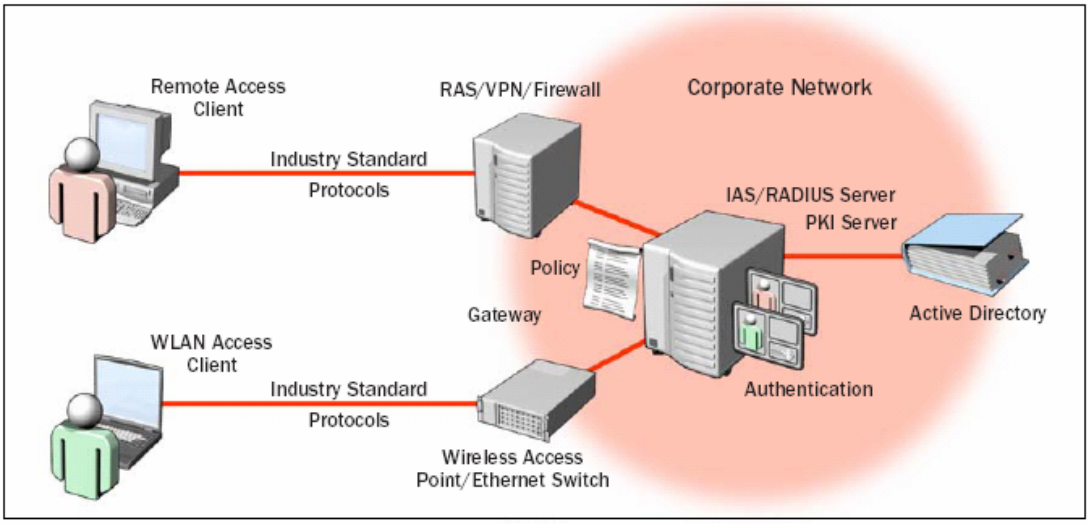

Figure 2. Windows Server 2003 Secure Network Access. (From Ref. [14].)

As depicted in Figure 1 and Figure 2, IAS/RADIUS can provide data confidentiality for the entire message and the attributes that are hidden. This is done by utilizing Internet Protocol Security (IPSec) with Encapsulation Security Payload (ESP) and an encryption algorithm such as Triple Data Encryption Standard (3DES). If none of the three security measures are possible, the following steps can be used to minimize the network vulnerability:

- Implement a Message-Authenticator attribute on all Access-Request messages.
- Deploy cryptographically strong Request Authenticators.
- Implement strong user passwords.
- Deploy an authentication count and lockout mechanism that will stop online dictionary attack against a user's password.
- Implement 128 bits of entropy for shared secrets. [Ref. 15]

Because the Message Authenticator attribute uses the shared secret, which can be weak due to poor configuration and limited size, the above steps will assist in decreasing those weaknesses of IAS/RADIUS if IPSec, ESP, and 3DES cannot be implemented. In addition, the shared secret is one of the hiding mechanisms that IAS/RADIUS uses. The Request Authenticator and the use of the Message Digest-5 (MD5) hashing algorithm are other mechanisms that encrypt user-password. The previous methods, viewed by the Internet Engineering Task Force (IETF), do not provide sufficient confidentiality protection to the passwords transmitted.

3. Secure Wireless and Ethernet Local Access Networks (WLAN/LANs)

Since the exponential growth of the Internet and its increased popularity and usage, many users are demanding a more secure access to the Internet whether via WLAN or LAN. In today's society, many networks are being targeted by hackers and malicious attacks. The security of these wireless and Ethernet LANs that are connected to the Internet is a necessity that can be provided by Windows Server 2003. The security measure can be met by implementing authentication and authorization of users. Using authentication and authorization methods has made improvements in wireless LAN security; Windows Server 2003 has accomplished this by supporting IEEE 802.1X protocols and PEAP. IEEE 802 is a standard defining the methods for accessing and controlling LANs [Ref. 16].

Today, 802.1X is the standard. “Based on the IEEE 802.1X specifications, improvements to Ethernet and wireless LANs facilitate secure authentication and authorizations of users and computers, regardless of connecting media.” [Ref. 17] But, the IEEE 802.1X is also concerned with connections across the wireless link and the methods used in protecting user data by scalable and secure management of data encrypted keys. The 802.1X specification recommends Extensible Authentication Protocol (EAP), as the protocol to be used in wireless authentication because of its widely used and flexible authentication transport. The 802.1X specification and EAP protocols are utilized in infrastructures such as those depicted in Figure 1 and Figure 2. As mentioned earlier, the IAS/RADIUS infrastructure has a RADIUS server that can authenticate client credentials. [Ref. 18]

There are many authentication methods EAP supports, such as Kerberos, Transport Layer Security (TLS), and Microsoft-Challenge handshake authentication protocol, which use a range of credential types such as passwords, certificates, one-time password tokens, and biometrics. Of course, any of these EAP protocols can be used for access to WLANs, but unfortunately not all of them are suitable to secure the WLAN. Currently, there are four principal EAP methods used for WLANs: EAP-TLS, PEAP, Tunneled TLS, and Lightweight EAP. Of the four principally used EAP protocols, PEAP and EAP-TLS are support by Microsoft. [Ref. 19]

PEAP is a two stage authentication, where the first establishes a TLS session to the server and permits the client to authenticate the server using the server’s digital certificates. The second stage uses an additional EAP protocol method tunneled inside the PEAP session to authenticate the client to the RADIUS server. An EAP-TLS protocol authenticates both the wireless clients and the RADIUS servers by establishing an encrypted TLS session between the two through the use of public key certificates.

EAP, a general protocol for WLAN data protection, and 802.1X provide several benefits:

- High security is achieved through authentication scheme that utilizes client certificates or user names and passwords.
- Strong encryption allows network data to have high strength encryption.

- Transparency enables a transparent authentication and connection to the WLAN.
- User and computer authentication provides separation of authentication for a user and computer where the computer can be managed even when no user is logged on.
- Network hardware is low in cost.
- High performance is attained because there is no impact on the performance level of the client computer due to the fact that the encryption is processed in WLAN hardware and not on the client computer. [Ref.19]

The above benefits of 802.1X provide an organization a secure WLAN that can overcome weaknesses discovered from the first generation of WLAN security. These weaknesses include flaws in security vulnerabilities, costly requirements of proprietary hardware, and security risks in virtual private networks. But, the technology of 802.1X with EAP has greatly improved wireless security where WLAN can deploy with a higher level of confidence in its security.

4. Software Restriction Policies (SRP)

In Windows Server 2003, SRP allows a systems administrator to set policies in order to prevent executable programs from running on a computer. The administrator can identify and specify certain software from untrusted code that can run in the organization's network environment. Figure 3 shows a general architecture of a software restriction policy that consists of three components:

- **Policy Is Defined for Domain Using Group Policy Editor -** The systems administrator creates the policy by utilizing the Group Policy Microsoft Management Console (MMC) snap-in for a particular Active Directory container site, domain, or organizational unit.
- **Policy Is Downloaded by Group Policy to Machine -** The policy is downloaded and applied to a machine, and user policies apply the next time a user logs on. Machine policies apply when a machine starts up.
- **Policy Is Enforced by Ooperating System When Software Is Run -** When a user starts a program or script, the operating system or scripting host checks the policy and enforces it. [Ref. 20]

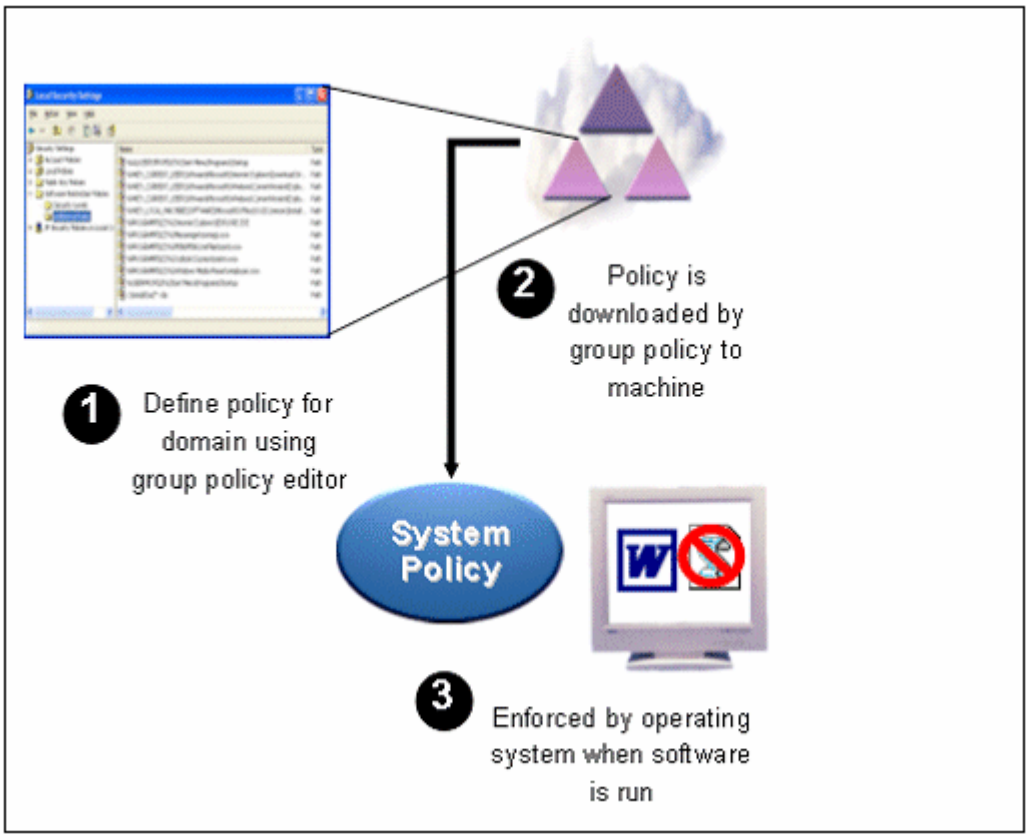

Figure 3. Three Components of Software Restriction Policy Architecture. (From Ref. [20].)

In setting the SRP, there are two default security levels. The default security levels can be defined as "Unrestricted" or "Disallowed" for a Group Policy; unrestricted permits the systems administrator to define exceptions that will allow a set of programs to run, and disallowed, a more secure approach, permits the systems administrator to specify only the programs that are known and trusted to run. There are four default security level exceptions that can be implemented: hash rules, certificate rules, path rules, and Internet zone rules. They are set by creating rules for specified software. [Ref. 20]

In a hash rule, malicious software can be prevented from running if a file has a virus or a Trojan horse. If a file compromises system stability, the hash rule, known as a cryptographic fingerprint, uniquely identifies the file. The file can be renamed or moved into another location on a disk and still have the hash rule match. The hash rule has three pieces of data that is separated by colons: MD5 or secure hash algorithm 1 (SHA-1) hash value, file length, and hash algorithm identification.

The certificate rule is a way of identifying software by specifying a code-signing and a software publisher certificate. This can be depicted by an organization mandating that scripts and ActiveX controls be signed with a particular set of publisher certificates. Certificates can be issued from a commercial source known as a certificate authority (CA) like VeriSign or a self-signed certificate [Ref. 20]. The certificate rule uses signed hashes contained in the signature of the signed file to match files regardless of name or location, but an exception can be made by using a hash rule to identify the exceptions.

In a path rule, a specific folder or fully qualified path to the program is created. The path rule will match any program contained in the folder and any programs contained in the subfolders, both local and Universal Naming Convention (UNC) paths are supported. In a particular example, a registry path rule can be used in looking up registry keys to many applications that store paths to their installation folders or application directories in the Windows registry. The locations of folders and application directories are not easily identifiable by using specific folder paths, but by creating a path rule and using the value stored in the registry this challenge is simplified.

Zone rules identify software that is downloaded from the Internet Explorer zone. The following zones included apply to only Windows Installer (*.MSI) packages: Internet, Intranet, Restricted Sites, Trusted Sites, and My Computer [Ref. 20]. Currently, the zones do not apply to software downloaded in Internet Explorer. When using this rule to install software from trusted Internet zone sites, the zone rule sets those trusted sites at an unrestricted setting.

5. Security Improvements for Servers on Ethernet and Wireless LANs

With the security improvements mentioned earlier in the "Secure Wireless and Ethernet LANs" section of this thesis, servers managing WLAN/LAN systems are reaping the security benefits as well. Due to the 802.1X authentication, port-based network access control provides authenticated network access for both Ethernet and IEEE 802.11 wireless networks [Ref. 21]. In order to effectively utilize IEEE 802.11, computer users must obtain valid certificates that can be managed by a RADIUS server on the wireless client. Both IEEE 802.11 and public certificates are supported by Windows server 2003, which allows computer systems to obtain certificates for authentication of WLAN/LAN connections. There are three ways to obtain certificates:

- **Using Auto-Enrollment of Computer Certificates -** This process automatically requests for and issues certificates based on Computer Configuration Group Policy. When Automatic Certificate Request Settings are configured, computers configured as a member of a domain system container will automatically request a certificate with specific parameters as the Computer Group Policy settings are refreshed.
- **Importing a Certificate File -** This method allows a certificate file to be created and distributed individually for each user. In addition, a single certificate can be sent to all users, known as a group certificate. Unfortunately, the group certificate is the least secure certificate deployment because any user obtaining the certificate file can use it to successfully authenticate a connection.
- **Using Internet Explorer and Web Enrollment To Request a Certificate from CA -** Basically, Internet Explorer can be used to request a certificate from a CA that supports Web enrollment for certificates. [Ref. 21]

Another medium for certificates is the use of smart cards that store the certificate in a micro-chip embedded in the card. This avenue is secure as long as the card holders maintain the cards on their persons. With these security improvements for servers, IEEE 802.1X and public certificates provide society with a secure means to use wireless in public places such as airports and malls.

6. Increased Web Server Security

Internet Information Services (IIS) 6.0, the Web server component, featured in Windows Server 2003 is far more secure than its predecessors IIS 4X or IIS 5X. IIS 6.0 has been redesigned with many new features to increase the security of an organization's Web infrastructure. What really makes IIS 6.0 and Windows Server 2003 more secure is that IIS 6.0 is in a locked-down state out of the box, with the strongest time-outs and content limits set by default [Ref. 22]. This lock down reduces potential attacks of the network system by closing the numerous security exploits and vulnerabilities. By turning off IIS 6.0 by default, this will force the systems administrator to explicitly select and install the built-in Web server. Other advanced security features of IIS 6.0, include: selectable cryptographic services, advanced digest authentication, and configurable access control of processes.

In redesigning IIS 6.0, an important new security feature in the built-in Web server is the new kernel-mode HTTP driver called HTTP.sys, which parses and queues

incoming HTTP requests and caches and returns application and site content. With the HTTP driver, this created a new type of logging called HTTP.sys logging, which helps determine the cause of attacks or potential attacks. This new process has HTTP.sys write to a log before a user's request is processed by IIS. If or when an error occurs during the process, such as if the process is terminated, the HTTP.sys error log will contain the request that caused the problem. [Ref. 23]

Authenticating a user during the logging process is important to having the Web server secure. Windows Server 2003 and IIS 6.0 ensure a secure log in process by using constrained delegation authority, also known as delegated authentication. Delegated authentication is the process that allows a Web server to utilize the credentials presented by a user in order to access other systems on the network. By using this authentication, systems administrators can help prevent attackers from arbitrarily using stolen credentials to access other systems in a domain. For example, if a user's credentials are compromised, the attacker can only access the applications selected by the administrators. This authentication is secure in Windows because the constrained delegation process does not pass the user's actual credentials to the server, which decreases the risk of a malicious administrator or application from stealing the credentials and later using them in an attack on the network.

In securing a user's credentials, the use of selectable cryptographic service allows a user to select a cryptographic service provider (CSP) that suits the user's needs. The CSP creates keys, destroys them, and uses them to perform a variety of cryptographic operations. Some CSP provide strong cryptographic algorithms, while others use hardware like smart cards. [Ref. 24]

Discussed later in more detail, Advanced Digest authentication is a mirror image of digest authentication except for the improvement of storing client credentials as MD5 hash in the Active Directory of the directory service in Windows Server 2003. This process makes it very challenging for hackers to discover users' passwords and does not require the administrator to modify the applications being used. [Ref. 25]

In configurable access control of processes, this security measure allows IIS 6.0 to better secure the Web server by configuring application pools. Basically, the identity of

an application pool has an account name that is used for the application pool's worker process runs. This account has a low-level user access rights that provides better security against attackers or malicious users who attempt to "hack" into the computer on which the World Wide Web Publishing Service is running. Systems administrators must be mindful not to give users increased user rights in order to prevent high security risk. [Ref. 26]

7. Encrypting the Offline Files Database

This feature is an improvement from the Windows 2000 Server where the cached files could not be encrypted. Systems administrators can now configure users' privileges in order to have encryption and decryption capabilities of an entire offline database.

How does encrypting work in Windows Server 2003? When data are encrypted, the user generates a request for a new security certificate identifying the requestor to the server. Then, a CSP generates two 56-bit keys: the public key used for encrypting data and a private key used decrypting the same data. The CSP passes the public key to the CA who uses it to create a certificate for the user. The certificate and the public key are stored in the Personal/Certificates folder located in the Certificates add-in to the Microsoft Management Console, shown below in Figure 4.

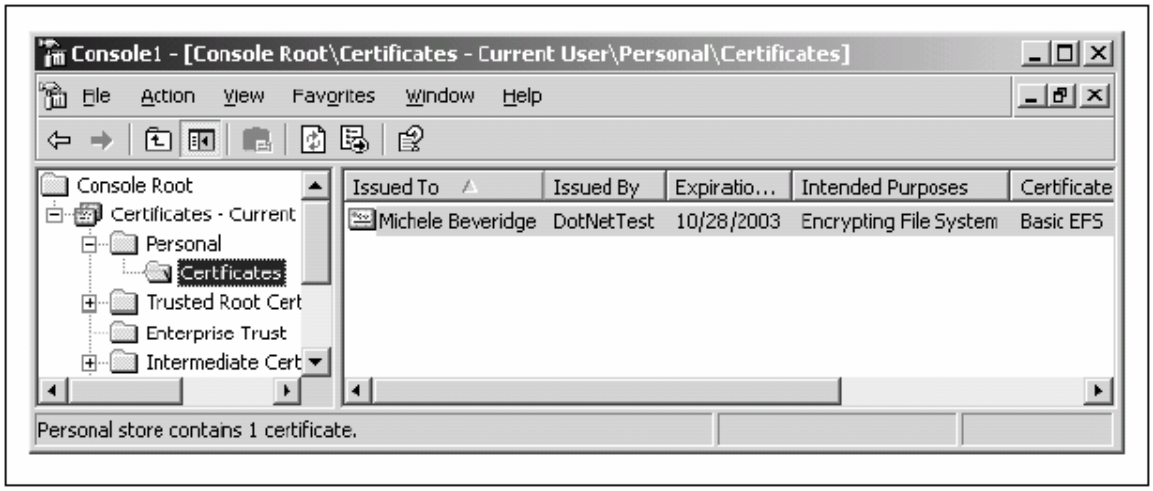

Figure 4. Personal Encryption Certificate. (From Ref. [1].)

8. Federal Information Processing Standard (FIPS) Compliant, Kernel-Mode Crypto Module

Federal Information Processing Standard (FIPS) is a standard or guidelines issued by the National Institute of Standards and Technology (NIST) for Federal computer

systems. FIPSs are developed when there is a compelling Federal government requirement such as security or interoperability and when there are no industry standards or solutions. Windows Server 2003 is compliant with FIPS 140-1, which provides a benchmark for implementing cryptographic software; later, Microsoft intends to submit cryptographic modules shipping with future operating systems for validation testing against FIPS 140-2, successor to FIPS 140-1. FIPS 140-2 is considered to be one of the most reliable industry standards that define security requirements for cryptographic modules. [Ref. 27]

There are four Microsoft cryptographic software components that have completed the FIPS 140-1 or FIPS 140-2 evaluation:

- Two Microsoft default cryptographic services providers.
- Windows Kernel-Mode Crypto Module.
- Exchange Cryptographic Services provider. [Ref. 28]

These components provide the cryptographic services required to secure a variety of protocols in numerous Windows Server 2003 features that include the following: Default CSPs and Kernel-Mode Crypto Module, Internet Explorer, and Public Key Certificate Server. The following are protocols whose cryptographic processing takes advantage of the components that have completed the FIPS evaluation:

- **Transport Layer Security Protocol -** Used between Web browser and Web server.
- **Internet Protocol Security Family of Protocols -** Used for end-to-end encryption.
- **Secure Multipurpose Mail Extension E-Mail Encryption Protocol -** Used to protect the confidentiality and integrity of e-mail messages.
- **Structured Query Language (SQL) Tabular Data Stream Protocol -** Used with Windows TLS/SSL Security Provider between SQL clients and SQL Server 2000 or above.
- **Microsoft Remote Desktop Protocol 5.2 or Above of Terminal Service Client -**Used to connect to a Terminal Server session on a Windows Server 2003.
- **Systems Management Server 2003 SP Management Protocol -**Used with Windows Active Directory for public key certificates repository and look up. [Ref. 28]

9. New Digest Security Package

With the numerous protocols designed for Internet security, Windows Server 2003 utilizes certain protocols to effectively create a secure gateway for clients. The new digest security package supports the new Advanced Digest authentication protocol, and includes support from Request for Comments (RFC) documents 2617 and 2222. In addition, these protocols are supported by a redesign of IIS and Active Directory service. The key feature in the package is the Advanced Digest authentication; this protocol stores the user credentials on the domain controller as an MD5 hash because the credentials are stored in Active Directory. This storage process does not allow the user passwords to be feasibly discovered by anyone with access to the domain controller. The steps in Figure 5 outline how a client is authenticated using Advanced Digest authentication.

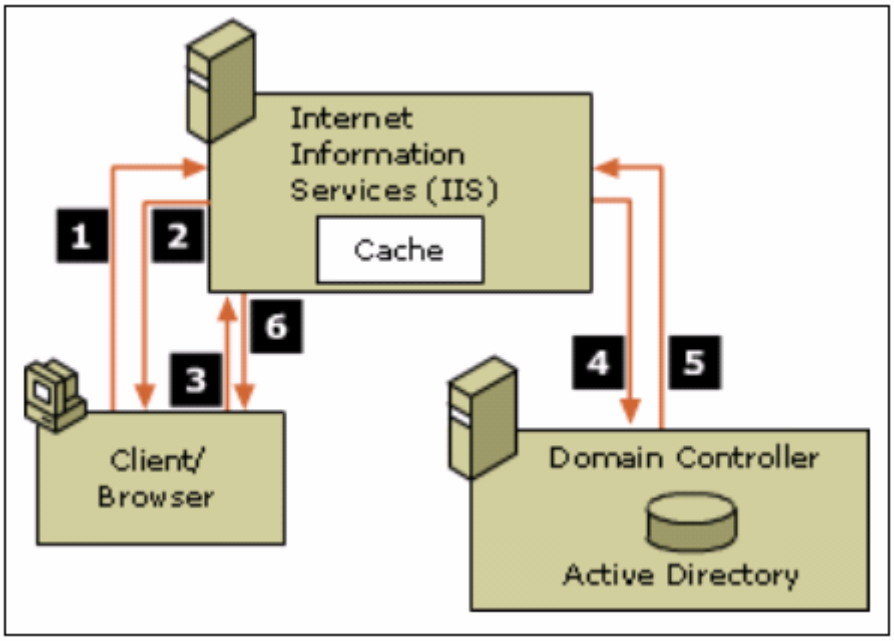

Figure 5. Client Authentication Using Advanced Digest Authentication. (From Ref. [29].)

Below are the steps in client authentication using Advanced Digest, as depicted in the figure above:

- Step 1 - The client requests a file from the server running IIS.
- Step 2 - The server running IIS denies the initial request and sends the client information; Digest authentication is being used as well as the realm name.

- Step 3 - The server running IIS reports to the client's browser that Digest authentication, rather than Advanced Digest authentication, is used because the same Digest authentication algorithm is used between the server running IIS and the client for both Digest and Advanced Digest authentication.
- Step 4 - The client's browser prompts the user for credentials (user name and password). The browser then combines these credentials with the name of the realm to create an MD5 hash and resubmits the request for the file to the server running IIS, this time also sending the MD5 hash in the header of the HTTP request.
- Step 5 - The server running IIS receives the client's hash and sends it to the domain controller for verification.
- Step 6 - The domain controller compares the client's hash to the copy stored in Active Directory. If the hash values match, the domain controller informs the server running IIS that the client is authenticated.
- Step 7 - The server running IIS sends the requested file to the client. [Ref. 29]

Although the new digest security package uses several protocols, there is no additional client software required when using Advanced Digest authentication. As defined by RFC 2617, Advanced Digest authentication relies on the HTTP 1.1 protocol, but, not all browsers support it. This limitation can result in non-HTTP 1.1 compliant browsers to be rejected when requesting a file from a server using Advanced Digest authentication.

10. System Security Improvements

As a whole, Windows Server 2003 has had a lot of security improvements, but in order to ensure overall system security, the secure socket layer's (SSL) performance was increased by over 35 percent [Ref. 16]. SSL is a means to encrypt communication between a client and a server computer. An example of encrypted communication is when an individual goes to a secure Web site desiring to transmit sensitive information. For example, a customer of a bank goes online to view an account, and obviously no one wants one's bank information to be intercepted by criminals or hackers. In order to encrypt a transmission between the customer's Web browser and the bank's Web server, a key exchange is made. This is done by the following steps:

- The customer's Web browser knows the bank's public key and uses it to encrypt the session key.

- The customer's Web browser then sends the encrypted session key to the bank's Web server, which uses its private key to decrypt the session key.
- The session key is decrypted by the bank's Web server, which can now be used to encrypt traffic between the customer's Web browser and the bank's Web server. [Ref. 1]

Basically, there is an agreement on a key to be used, one side (client computer) encrypts a suggested session key with the recipient's (server computer) public key, and the recipient is able to decrypt without anyone being able to snatch the session key as it travels the wire via the Internet. This process has definitely secured communication between the client and the server computer during transmission of data.

As mentioned earlier, the re-design of IIS improved security by having systems administrators to set the service when the organization is ready to deploy IIS. This, not installed by default setting, protects network systems from hackers attempting to gain access that was open in the Windows 2000 Server operating system. Another improvement in system security is Microsoft Visual Studio's capability in buffer checking which limits the exploited buffer overruns commonly used by hackers.

11. Credential Manager

The functions of the Credential Manager are to request account information and to allow users to log on. Credentials Management Application Programming Interface (API) and Credentials Management User Interface in Windows Server 2003 are used to obtain and manage credential information such as user names and passwords. The Stored User Names and Passwords featured in Windows Server 2003 is able to associate a set of credentials with a single Windows user account, using Data Protection API (DPAPI), which is used in place of the credentials being established while logging on [Ref. 30]. This process occurs when the log-on credentials do not have the required permissions by the application.

How is DPAPI used? DPAPI is a password-based data protection service, in Windows Server 2003, that requires a password to provide protection. The API uses a pair of function calls to provide the operating system data protection services to the user and system processes. Since this data protection is part of the operating system, every application can secure data without needing specific cryptographic code other than the function calls from DPAPI. Although the DPAPI protection relies on the password

provided, this weakness is offset by DPAPI's use of proven cryptographic routines, such as Triple-DES algorithm and strong keys. [Ref. 30]

12. Share Permissions

Share permissions in Windows Server 2003 are the most fundamental form of access control a systems administrator can manage. Share permissions are like an access pass a person receives when trying to enter a secure building. When a person walks up to the front door and shows identification, the guard looks at the individual's name and gives the person a pass that signifies the access level for everything inside the building. Such as, if the pass specifies a level one access, then the individual with the pass has access to level one access. This process is similar to share permissions where this feature allows systems administrators the capability to assign access levels to users.

Systems administrators should keep in mind that share-level permissions only represent the maximum level of access an individual will get on the inside. Basically, if a user is given read permissions at the share, the most the user can do once connected remotely to the share is read. But, understand that even if a user has full control at the share, the object inside can still have NTFS (New Technology File System) permissions that can specify the user to have only read permissions. [Ref. 1]

When defining share permissions, the systems administrator will use the Computer Management Console and select the share to secure by right-clicking the share name and selecting Properties, then selecting the Share Permissions tab. Figure 6 shows the Share Permissions tab. From the figure, the Everyone group has Read access permissions by default. This default setting is an improvement to security for the Windows Server operating systems considering that operating systems prior to Windows Server 2003 had given the Everyone group Full Control access by default. In addition, the Everyone group no longer contains the Anonymous User account which will help keep an organization's resources more secure.

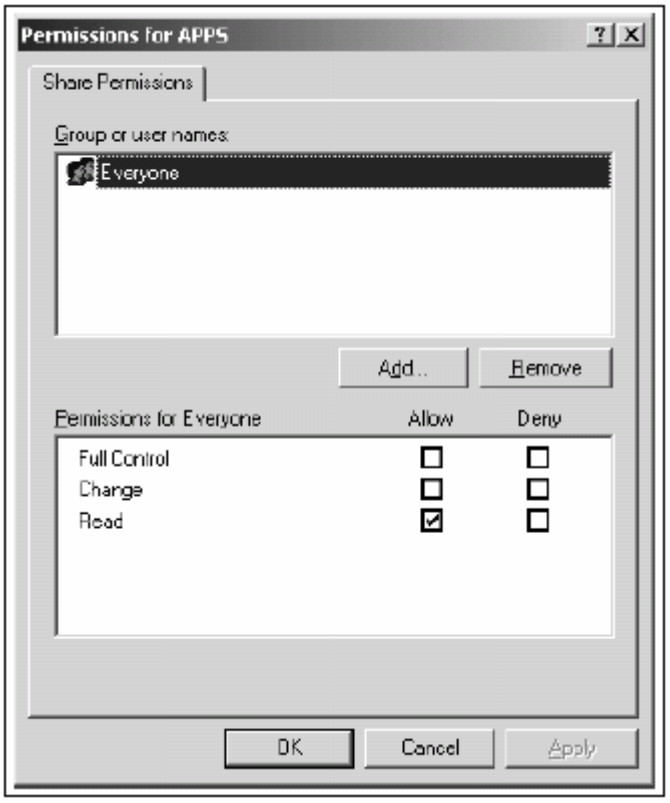

Figure 6. Share Permissions Tab. (From Ref. [1].)

13. SSL Client Authentication Improvements

SSL client authentication improvements have enabled Windows Server 2003 to share the SSL session cache by multiple processes. This improvement makes the system more efficient by reducing the number of CPU cycles on the application server and the number of times a user has to re-authenticate with applications. [Ref. 16] As stated earlier, SSL is a means of securing communications between a client and a server computer; Windows Server 2003 has effectively optimized the use of SSL in authenticating users and its ability to transmit and receive sensitive data in a secure medium.

B. DEPLOYMENT OF PUBLIC KEY INFRASTRUCTURE

Windows Server 2003's trustworthy computing will make it easier for organizations to deploy a public key infrastructure (PKI) in tandem with associated technologies such as the common access card or smart card. Recently, organizations have seen the need to communicate with employees from afar. Many personnel frequently travel and must maintain a connection with their companies in order to get the

job accomplished. In Windows Server 2003, public key infrastructure has made the gateway to the Internet a more secure connection by using the PKI features of certificate auto-enrollment and auto-renewal, Windows Installer Digital Signature Support, and Certificate Revocation List. These features and other improvements give the systems administrator more flexibility to manage authorized users to access the organization's network.

1. Certificate Auto-Enrollment and Auto-Renewal

In the previous Microsoft operating system, Windows 2000 Server had the capability to auto-enroll for Encrypted Files System certificates and computer certificates, but, it did not have the functionality to auto-enroll users. This new feature, certificate auto-enrollment for users, in Windows Server 2003 has improved both the user and computer enrollment experience. For instance, an account member of an Enterprise Admins group can specify the types of certificates that an entity should automatically be issued. The Enterprise group administrator can easily manage and control auto-enrollment by setting security permissions on certificate templates that are built in the Certificate Templates snap-in. Basically, a Windows XP or Windows Server 2003 family client that is granted access can enroll the certificate templates by accessing the templates in the Active Directory directory service.

The certificate auto-renewal feature is very similar to the auto-enrollment feature. Both features use the same mechanism to access the templates that are used to control who can auto-renew a certificate. This process allows every certificate in the certificate store that has a template extension to be potentially auto-renewed by the system. Auto-renew gives the system a means to prevent an application's certificate from expiring.

To assist administrators with the burden of managing certificates, below are some enhanced certificate management tools in Windows Server 2003 certificate services:

- **Certification Authority (CA) Microsoft Management Console (MMC) Snap-In -** This tool enables the administrator to configure CA component running on Windows Server 2003.
- **Certificate Templates MMC Snap-In -** Feature operates in the same manner as it did in Windows 2000; it allows an administrator to view certificate store for user, service, and computer accounts.

- **Certificate Templates MMC Snap-In -** This is a new feature in Windows 2003 that allows the administrator to clone and edit Certificate Templates, a capability not available in the previous operating system.
- **Command Line Utility (CERTUTIL) -** The versatility of CERTUTIL is at the command prompt. This feature displays a long list of available options and functions in CA management. [Ref. 31]

2. Windows Installer Digital Signature Support

Windows Installer version 2.0 inside Windows Server 2003 supports the use of digital signatures that will detect corrupted resources during installation. Windows Installer has been designed to install files in a package where components are independent. Microsoft has focused on installing file standards that will improve the successful installation of files to be undone, in comparison with most uninstalls that have been done in the past [Ref. 1]. This feature will definitely cut time on reworking installations and debugging files.

The digital signatures support in version 2.0 can be used with Windows Installer packages, transforms, patches, merge modules, and external cabinet files. Stated earlier, this process will allow a package author or administrators to have confidence that the installation processes of files are being installed properly and that none of the files were corrupted. Important to note is that the digital signature support does not provide the ability for a package to automatically be run with elevated permissions. [Ref. 32]

3. Certificate Revocation List (CRL) Improvements

The use of PKI and certificates has greatly improved the process of verifying users and computers to one another by issuing certificates. But, what happens when a certificate is no longer in use or a certificate associated with a laptop is stolen? These two situations require the certificates to be revoked from the list of the issuing CA. Actually, a certificate revocation is issued by the CA in the form of a list. The CRL can be fairly large, and publishing a new version on a frequent basis can use a lot of network bandwidth. This replication process places a load on clients who require the download. To improve the process, the concept of Delta CRL was introduced.

The Delta Certificate Revocation List in Windows Server 2003 can be issued on a regular basis, by default weekly, but it can be issued more or less often. This new feature is an improvement over the previous CRL because the Delta CRL contains only the

update changes in the revocation status of certificates that have been made since the last published list. This new concept has prevented the republishing of an entire CRL with changes made, which would be an enormous file to be downloaded, and has improved processing time by decreasing replication traffic and usage of network bandwidth. [Ref. 33]

C. SECURE EXTENSION OF AN ORGANIZATION TO THE INTERNET

Today, organizations are seeking ways to secure their communication with employees, customers, and partners who are not located within its intranet. Windows Server 2003 will make securing extended access to the network more transparent to all users, whether individual or other organizations accessing data or other resources within the intranet. In order to beat the competition, an organization's need to connect its own personnel to their intranet is increasing as much as the number of people who connect to the World Wide Web Internet. A solution to this dilemma is to provide access to other personnel through the use of Passport Integration and Cross-Forest Trusts.

1. Passport Integration

There have been numerous security improvements in the use of Internet Information System that have made accessing the Internet from outside the intranet more secure. Passport integration is another feature that can be used to increase secure connectivity to the network by integrating Windows Server 2003 IIS 6.0 with Passport. This process allows Passport identities to be authenticated in the core Web server and gives the systems administrator the capability to authorize a user to perform a certain task. Through the integration of Passport and IIS, Passport integration can act as a Web application that can authorize URLs together with the IIS Authorization Manager feature, and will also give administrators better access control. [Ref. 34]

Passport integration with IIS 6.0 provides better access control due to the interfaces in the standard components package of Passport version 2. As soon as Passport gives authorization to the user, the systems administrator can map the user to an Active Directory for increased credential dispersion. This feature provides an equivalent single sign-on experience using IIS without having to log-on directly to a Windows network.

2. Cross-Forest Trusts

Recall, what a trust is? The network administrator creates a trust relationship between two domains who desire to connect to each other whether an old or new domain. The trust can also be one domain in one forest to trust domains in another forest. When a laptop or workstation joins a domain, the laptop or workstation is willing to accept authentications from its own domain controller and from the second domain controller. As for a forest trust, this trust relationship is a multi-domain structure of an enterprise that is comprised of multiple tree domain structures.

Forest trust is a new type of Windows trust for managing the trust relationships between two forests. The Active Directory in Windows Server 2003 makes managing multiple forests and cross-domain trusts much easier. This feature significantly simplifies the cross-forest security administration and enables the domain controller of the trusting forest to enforce constraints on specific security domain names that it trusts other forests to authenticate. [Ref. 35]

For instance, organizations with multiple forests or the organization that has a trusted partner that also has a forest can easily have the systems administrator set up one transitive trust between the two forests instead of creating trusts between each separate domain in each forest. Both forests must have Windows Server 2003 forest functionality mode running to utilize this feature.

Hence, cross-forest trust gives the administrator the ability to set permissions that are based on the users or groups residing in the other forest. Once the permissions are set, the Active Directory allows the authentication and authorization between the two forests to take place across the forest boundaries.

D. CHAPTER SUMMARY

Microsoft's vision of providing "trustworthy computing" has really started off well with the redesign of Windows Server 2003. This new operating system has had a major overhaul; especially, the security aspect of the operating system that has been improved to increase the secure connectivity of personnel and customers in an organization. Windows Server 2003 is a more secure operating system than previous Microsoft operating systems.

With a secure platform, a better means of deploying a public key infrastructure, and a secure extension for external personnel to connect via the Internet, Microsoft's Windows Server 2003 provides users and administrators a more secure medium to access networks and other company IT resources. Features in the new operating system, ranging from the Internet Connection Firewall to the Secure Socket Layer client authentication, have enabled users the benefit of working aboard with less worries from hackers or viruses impeding productivity. In addition, the improved deployment of public key infrastructures and the secure extension to the Internet have made it easier for administrators to manage certificates.

The numerous improvements such as the ICF, IAS, and IIS have alleviated many of the headaches associated with securing a network enterprise. During the development of Windows Server 2003, Microsoft changed their processes and produced a product that is "secure by design, secure by default, and secure in deployment." Thus, Windows Server 2003 is a great improvement from previous operating systems. Windows Server 2003 will be an asset to an organization's network system not because of its popularity, but because of its security features and improvements.

III. WINDOWS SERVER 2003 EDITIONS AND FEATURES

Windows Server 2003 was designed to simplify the administrator's task of deploying and managing the operating system, by building on the best of Windows 2000 Server technology. "Windows Server 2003 is one of the industry's most advance operating systems, and supports high levels of performance, reliability, availability and manageability for enterprise environments." [Ref. 36] These new operating systems offer organizations' IT staff infrastructure the leverage to be more dependable, to be more productive, and to stay connected. [Ref 3] This chapter discusses Windows Server 2003's capabilities in handling a multitude of server roles varying from centralized to distributed means and other features that provide the dependability and connectivity to personnel and customers. The new and enhanced features will be introduced and discussed in more detail within the context of Windows Server 2003.

A. WINDOWS SERVER 2003 FAMILY EDITIONS

The Windows Server 2003 family consists of five editions: Standard, Enterprise, Datacenter, Web, and Small Business. Table 1 gives a brief description of the individual server editions. The Standard edition is groomed for departmental and standard workloads, while the Enterprise and Datacenter editions are for those organizations seeking the highest availability and scalability for network systems. The Web edition provides companies with servers that are dedicated to Web serving and hosting, and the Small Business edition basically offers a secure and reliable IT infrastructure. These five editions are different in the various capabilities and functionalities, but share the core technology. [Ref. 37]

WINDOWS SERVER 2003 FAMILY EDITIONS

Product	Description	Key Features
Windows Server 2003, Standard Edition	Designed for departmental and standard workloads and delivers the following: support for file and printer, more secure Internet connectivity, and centralized desktop application deployment.	Common Language Runtime XML Web services Active Directory Internet firewall Remote access Shadow Copy of Shared Folders Terminal Server Internet Information Service Wireless LAN support Server event tracking
Windows Server 2003, Enterprise Edition	Built for mission-critical server workloads and is the platform of choice for applications, Web services, and infrastructures.	All Windows Server 2003 Standard features Eight-way symmetric multiprocessing (SMP) Eight-node clustering Up to 32 GB of RAM Meta-Directory Services Support
Windows Server 2003, Datacenter Edition	Built for the highest levels of scalability and reliability, and the most powerful and functional server operating system Microsoft has ever offered.	All Windows Server 2003 Enterprise features 32 way SMP 64 GB of RAM Intel Hyper-Threading Non-Uniform Memory Access (NUMA)
Windows Server 2003, Web Edition	Operating system dedicated to Web serving and hosting Web applications, Web pages, and XML Web Services. Designed primarily as an IIS 6.0 Web Server.	Dedicated Web Server, therefore has limited functionalities compared to other editions. Up to 2 GB of RAM 2-way SMP
Windows Small Business Server 2003	Integrates a suite of server products to enable companies to share information and resources safely and securely. (Standard and Premium editions)	All Windows Server 2003 Standard features Web Standard: - SharePoint Services - Exchange Server - Shared Fax Web Premium: - All features of standard - Internet Security and Acceleration SQL FrontPage

Table 1. Windows Server 2003 Editions and Features. (After Ref. [37].)

In addition to the features listed in Table 1, the Windows Server 2003 Editions and feature highlights are compared in the set of tables depicted in Appendix A. The set

of tables are broken down into functions and provide a quick comparison of the capabilities in the different editions. This section will discuss feature highlights in Windows Server 2003 editions.

1. Windows Server 2003 Standard Edition

Windows Server 2003 family is a platform that allows organizations to leverage all the functionalities within the operating system. As mentioned earlier, the core technology of Windows 2000 Server has been the design foundation that made Windows Server 2003 a more secure, reliable, available, and scalable operating system. Illustrated in Table 1 and the set of tables in Appendix A, Windows Server 2003 has numerous features and functionalities; the Windows family is a multipurpose operating system capable of supporting various functional needs of an organization that can connect information, people, systems, and devices. The new and improved features in the Windows Server 2003 family provide the means to handle a diverse set of server tasks.

Windows Server 2003 provides dependable systems with numerous features such as Active Directory (AD) service. AD, to be discussed later in this chapter, is an important feature that has been designed faster and more robust in unreliable wide area network connection. The 2003 operating system provides improved connectivity through features like its Web service, which makes it easier for organizations to share information among partners, customers, and employees over the intranet, the Internet, or via an extranet.

Windows Server 2003 System Requirements				
Requirement	**Standard Edition**	**Enterprise Edition**	**Datacenter Edition**	**Web Edition**
Minimum CPU Speed	133 MHz	• 133 MHz for x86-based computers • 733 MHz for Itanium-based computers*	• 400 MHz for x86-based computers • 733 MHz for Itanium-based computers*	133 MHz
Recommended CPU Speed	550 MHz	733 MHz	733 MHz	550 MHz
Minimum RAM	128 MB	128 MB	512 MB	128 MB
Recommended Minimum RAM	256 MB	256 MB	1 GB	256 MB
Maximum RAM	4 GB	• 32 GB for x86-based computers • 64 GB for Itanium-based computers*	• 64 GB for x86-based computers • 512 GB for Itanium-based computers*	2 GB
Multiprocessor Support **	Up to 4	• Up to 8	• Minimum 8-way capable machine required • Maximum 64	Up to 2
Disk Space for Setup	1.5 GB	• 1.5 GB for x86-based computers • 2.0 GB for Itanium-based computers*	• 1.5 GB for x86-based computers • 2.0 GB for Itanium-based computers*	1.5 GB

* **Important:** The 64-bit versions of Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition are only compatible with 64-bit Intel Itanium-based systems. They cannot be successfully installed on 32-bit systems.

** Windows Server 2003 may not use multiple processors with some Intel Pentium Pro or Pentium II Processors.

Table 2. Windows Server 2003 System Requirements. (From Ref. [38].)

Staying connected with the world, Windows Server 2003 is like any system; it has minimum requirements. The system requirements for the operating system depend on the organization's selection of family editions and the degree of performance at which the network system is desired to be functioning. Table 2 above shows the system requirements for each of the Windows Server 2003 family editions.

Generally, faster is better; but, Windows Server 2003 will operate with a system CPU speed of 266MHz [Ref 1]. Of course, 1 GHz or 2 GHz is better, provided the system has sufficient amount of RAM. RAM is another important system requirement that helps improve the high performance of a server.

Referring back to Table 1, the Business edition is not included because it utilizes the Standard edition, and, therefore, it has the same system requirements as the Standard. Depending on what the organization's infrastructure and business needs are, it will determine what system requirements are optimal in deploying the Windows Server 2003 edition.

2. Windows Server 2003 Enterprise Edition

Windows Server 2003 Enterprise edition is designed for high performance servers and supports the capability to cluster servers for better load handling. These capabilities are the primary difference between the Enterprise and Standard editions. The Enterprise edition provides greater availability, scalability, and dependability due to the enhanced features from Windows 2000 Server technology, such as network load balancing, server clusters, and Active Directory Services. The following improvements in Windows Server 2003 are also included in the Datacenter edition: Cluster Service, Multiprocessor support, Meta-Directory Services support, Hot Add Memory, Non-Uniform Memory Access (NUMA), Terminal Services session directory, and Windows System Resource manager. Theses improved features support demanding servers and provide a high performing network.

a. Cluster Service

Windows Server 2003 Cluster Service offers increased availability and disaster tolerance for essential database management, file sharing, intranet data sharing, messaging, and general business applications. Many organizations confront issues that involve unexplainable downtime, but no matter the cause of the failure, systems administrators are responsible for the system "crashing." Clustering technology used in Windows Server 2003 Cluster Service provides improved availability and scalability for systems that have stringent requirements. This section will discuss Windows Server 2003 clustering features that consist of two different technologies: Server Cluster and Network Load Balancing (NLB).

(1) Server Cluster. Server Clusters are primarily used to increase availability for mission critical applications through fail-over. Fail-over is when a server automatically switches to a redundant or standby server upon the failure or abnormal termination of the currently active server. This occurs without any human intervention. Server Cluster is an improvement, from Windows 2000 Advanced Server and Datacenter Server, of the Microsoft Cluster Service component. In order to deploy Server Cluster, the systems administrator must configure between two and eight servers to act as nodes in the cluster. Next, the cluster resources (i.e., network names, IP addresses, applications, services, and disk drives) are configured, which is required by the

applications being clustered. These resources are assigned to one cluster node at a time. When a Server Cluster detects a failure of primary nodes for a clustered application, or the node is offline due to maintenance, the clustered application is started up on a backup cluster node. Any requests from the clients are redirected to the backup cluster nodes in order to minimize the impact of failure.

The nodes in a cluster utilize a quorum, known as a storage device to manage the nodes owning an application. There are two types of quorums: single quorum device server cluster and majority node set server cluster. The quorum is controlled by the primary node for the clustered applications. Similar to an application that can only be assigned one node, only one node may own a quorum at a time. If an application fails over to a backup node, the backup node has ownership of the quorum. Figure 7, illustrates an example of a single quorum device that shows all the nodes connecting to a single storage device. This architecture simplifies the challenge of transferring control of the data to a backup node. Unfortunately, this architecture is weak because if the storage device fails, the entire cluster fails. In addition, if the storage area network fails, whether from floods, fires, earthquakes, and/or other serious problems, again, the entire cluster fails. Therefore, the single quorum device server cluster is not the best solution for an organization that requires continuous work even if the physical facility is taken offline. Other means of redundancy are required.

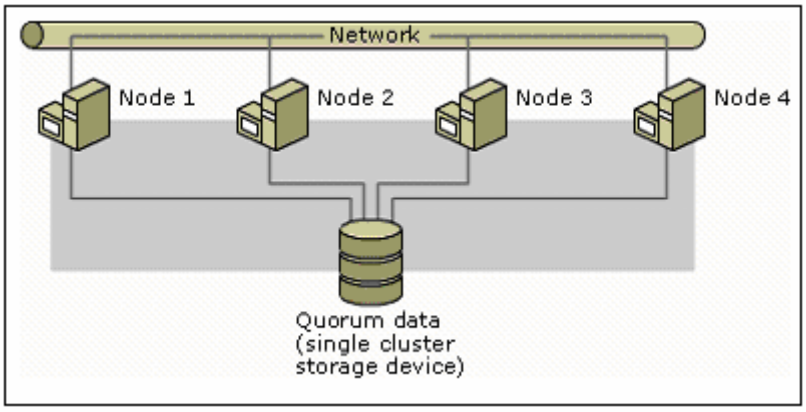

Figure 7. Single Quorum Device Server Cluster. (From Ref. [39].)

In the majority node set (MNS) server clusters, the quorum stores on a locally attached storage device that connects directly to each cluster node. As for the backup node, it must have a copy of the data stored within the quorum in order to take

control of the quorum. The server cluster manages this process by replicating quorum data across the network. Figure 8 shows that the MNS cluster nodes are connected by the network. This architecture does not specify the type of network, but, the network can be a local area network, or wide area network, or even a virtual private network. The network used connects the cluster nodes in different buildings or cities, which allow a cluster to overcome any geographical restrictions imposed by the storage connections.

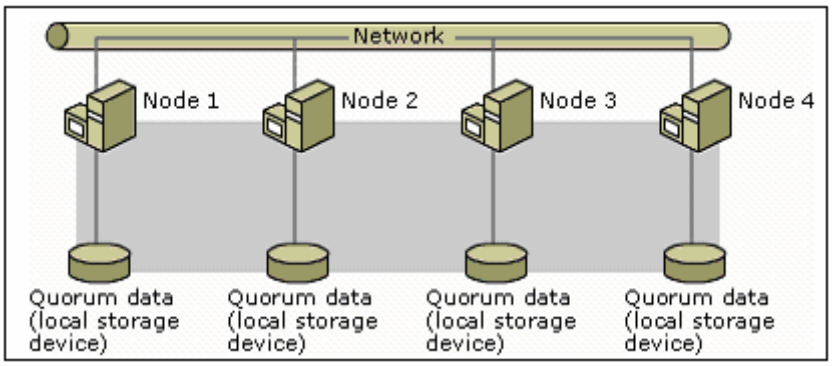

Figure 8. Majority node set server cluster. (From Ref. [39].)

For MNS clusters to effectively fail over, MNS server clusters require at least three nodes, and more than half of the cluster nodes in the server cluster to be active at all times. For a three node MNS server cluster, two of the three nodes must be active. In an eight-node MNS server cluster, there must be five nodes active to remain online. In contrast, the single quorum device server clusters requires only one node to be active in order for the server cluster to remain online.

(2) Network Load Balancing (NLB). Network Load Balancing is the second clustering technology used in Windows Server 2003. NLB cluster allows the systems administrators to take two or more computers and make them look like one computer to the end users. It is different from using the quorum because NLB does not impose storage or network requirements on the cluster nodes. The two or more computers of the NLB cluster each have their own static IP address and allows everyone of the NLB cluster members to take the same IP address. The sharing of IP addresses should hinder the communication between the two systems, but with NLB, it fixes this by assigning each visitor a specific cluster node. When a node in the cluster fails, the NLB server cluster will automatically redirect incoming requests to the remaining nodes.

Figure 9 shows an example of a NLB that is most often used to build redundancy and scalability for firewalls, proxy servers, or Web servers. NLB clusters can scale up to 32 nodes, and be clustered with VPN endpoints, streaming media servers, and terminal services.

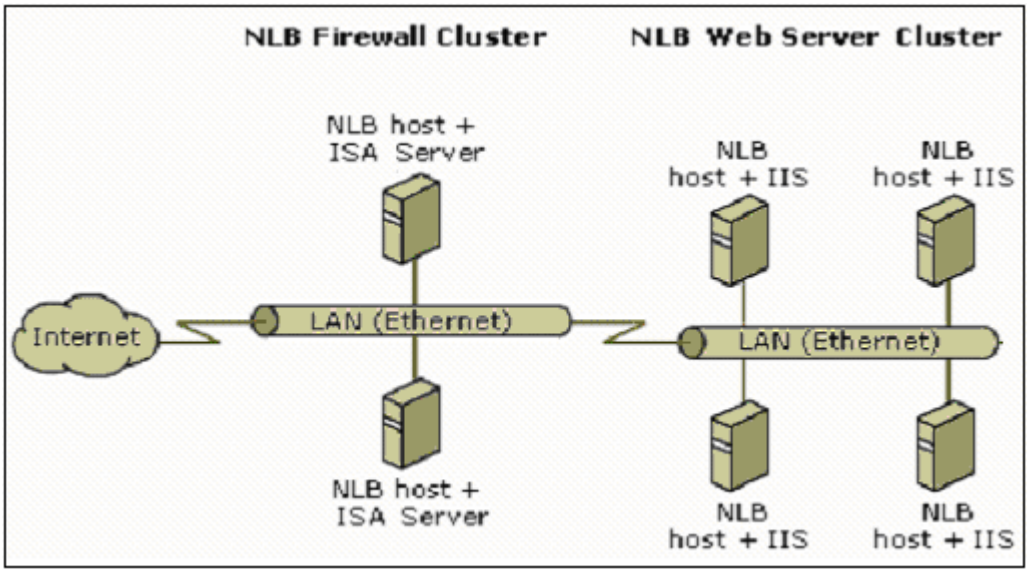

Figure 9. Network Load Balancing Cluster. (From Ref. [39].)

b. Multiprocessor Support

Windows Server 2003 supports single or multiple central processing units that comply with symmetric multiprocessor (SMP) standards. SMP is a set of processors that share a common pool of memory that must be equally accessible to each of the processors. By utilizing SMP, Windows Server 2003 can use multiple processors for applications that require additional processing power. This capability is possible because the operating system is capable of running threads on any available processor. In contrast to asymmetric multiprocessing, systems will allocate resources to a specific processor even if the central processing unit is overloaded, while other processors are relatively free of tasks. Thus, there is a clear advantage to multiprocessor support that provides the capability to balance processing load across all of the computing resources in a system.

c. Meta-Directory Services Support

Microsoft Meta-Directory Services (MMS) provides a means to manage and integrate personnel's identity information from multiple directories, databases, and files with Active Directory. As information increases exponentially, the infinite amount of data in an organization must be managed; in particular, the information flow and

relationships among workers within an organization, the relationships to customers and business partners, and the internal business processes generate an abundance of identity information that needs to be managed and integrated. With Windows Server 2003, MMS gives administrators a unified view of identity information, enables the integration of business processes with MMS, and helps synchronize identity information across an organization. This process resolves organizations from having information stored in multiple and different data repositories throughout the organization.

As with any imperfect application, Microsoft Meta-Directory Service has a flaw. This flaw is an authentication vulnerability that could enable an unprivileged user to access and manipulate data within MMS. The unprivileged user can connect to the MMS data repository by using a Lightweight Directory Access protocol client and be able to bypass certain security checks. In doing this, the attacker can modify data within the MMS data repository. Systems administrators can download and apply the Microsoft Meta-Directory Services 2.2 Service Pack 1 at Microsoft's Web site (http://download.microsoft.com/download/mms22/Patch/Q317138/NT5/EN-US/Q317138.EXE), which addresses the vulnerability. [Ref. 40]

d. Hot Add Memory

Hot Add Memory (HAM) is supported by Windows Server 2003 Enterprise and Datacenter editions. This application allows ranges of physical memory to be added to a server that has a running operating system, without requiring the system to reboot. HAM's capability minimizes a common source of downtime for a network. The need to power-off the server, and thereafter, rebooting the system during memory upgrades are nothing but in the past due to HAM. Basically, Hot Add Memory will allow administrators to add memory to a running system without shutting down whenever a need for increased memory exists.

Currently, the Hot Add Memory feature operates only on systems where hardware supports are in place for adding memory while the server is operating. Microsoft has required systems manufacturers to configure their hardware in the following way in order to support Hot Add Memory:

- Implement a mechanism for adding physical memory regions to an operating system instance without a system power operation.

- Design the BIOS to describe Hot Add Memory accurately to the operating system. [Ref. 41]

To ensure platforms interoperated with Windows Server 2003, Microsoft had the systems manufacturers provide a test platform for the Windows development labs, which would in turn conduct the appropriate test to verify the test platform's interoperability with Windows Server 2003.

e. Non-Uniform Memory Access (NUMA)

Windows Server 2003 supports multi-processing and a traditional model; it is a symmetric multiprocessor (SMP). This model allows each processor to have equal access to memory and to input/output. When the administrator adds more processors to the system, the processor bus of the system becomes a limiting factor to the entire network's performance. To resolve this issue, Non-Uniform Memory Access is utilized to increase processor speed without increasing the load on the processor bus. NUMA's architecture was designed as non-uniform because each processor is close to some parts of memory and farther from other parts of memory. In essence, the processor will quickly gain access to the memory that is closest to it, versus trying to access memory farther away, to which it would take longer to gain access.

Systems utilizing NUMA will improve performance through the process of directing threads on processors that are on the same nodes as the memory. Of course, the systems will allocate memory from other nodes if necessary, but it will attempt to satisfy memory allocations first from within the same nodes. NUMA enhances the performance of applications by optimizing the scheduling and usage of memory.

As mentioned earlier, the NUMA architecture helps prevent the system buses from creating a bottleneck by supporting an optimal number of processors. Figure 10 shows a NUMA architecture that consists of two four-processor NUMA nodes that are connected as an eight–processor NUMA system.

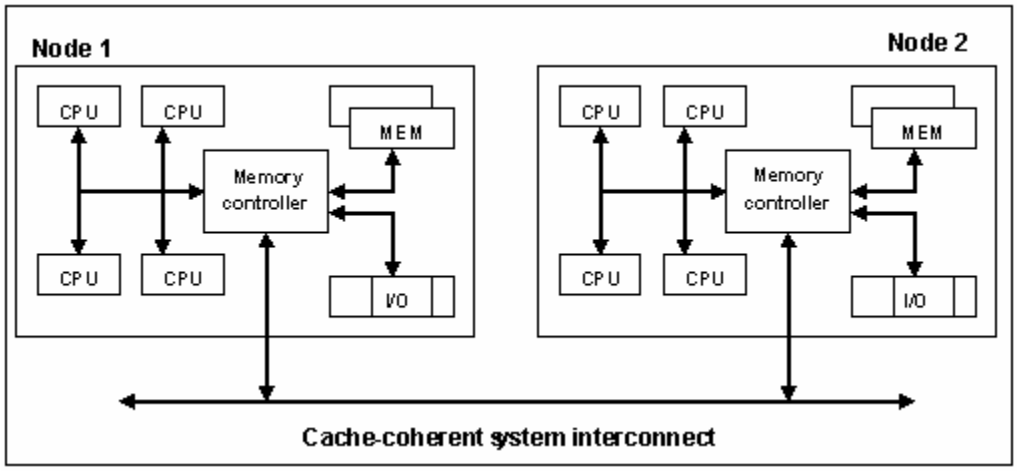

Figure 10. Two Four-Processor NUMA Nodes Connected as an Eight-Processor NUMA System. (From Ref. [42].)

Furthermore, each node contains processors, memory, and I/O; these resources within the node are all considered to be local. When the system accesses memory within the node, this process is called "uniform." As seen in the figure above, the nodes are connected by a high-speed cache-coherent system made of symmetric multiprocessors. When the system accesses memory in another node rather than accessing the local memory, the delta time in accessing the memory is called "non-uniform." The delta time is referred to as the NUMA ratio; the higher the NUMA ratio value tends to have a greater affect on software performance. To ensure optimal performance of the system, the NUMA ratio is recommended to be no greater than three to one (3:1). [Ref. 42] The NUMA feature is useful to users who rely on maintaining connectivity to network resources without losing performance in the system buses.

f. Terminal Services Session Directory

Session Directory technology used in Terminal Services allows a user to reconnect its Terminal Services session whenever a connection has been disconnected. Terminal Services Session Directory service is a database that monitors user sessions on the terminal servers in a load-balanced cluster. This feature provides information that is used during connection time in order to connect the user to an existing session. The Terminal Servers in a load balanced environment can be organized in a group, also known as a farm. The Session Directory database can reside on a server outside the farm, but it is possible for a user to be on a member of a farm. [Ref. 43]

As mentioned earlier, the Session Directory database records user names associated with the session's identification that is connected to the servers in a load-balanced Terminal Server farm. With this information, the Terminal Service's load balancing pools the processing resources of numerous servers by utilizing the TCP/IP networking protocol. In addition, the systems administrators are able to use a cluster of terminal servers and scale the performance of a single terminal server through the distribution of sessions being processed by multiple servers.

Terminal Services Connection Management (TSCM) is a management tool that monitors the disconnected sessions that are on the cluster and ensures users are connected to the user's disconnected sessions on the same server. This monitoring process conducted by the TSCM is briefly described by following five steps:

- Step 1- When the user logs on to the Terminal Server Cluster, the terminal server receiving the initial client log-on request sends a query to the Session Directory server.
- Step 2 - The Session Directory server checks the user name against its database and sends the result to the requesting server.
- Step 3 - If the user has no disconnected sessions, the log-on process continues at the server that is hosting the initial connection.
- Step 4 - If the user has a disconnected session on another server, the client session is passed to the second server and the log-on process continues from that point.
- Step 5 - When the user logs on to the disconnected session, the Session Directory is updated. [Ref. 44]

To reiterate the process of the Session Directory, the service has three basic requirements to have a system running properly. Those requirements are listed below:

- A network load-balancing solution such as Network Load Balancing, Domain Name Service round-robin, or a third-party solution.
- Two or more terminal servers logically grouped into a terminal server cluster.
- A Windows Server 2003 computer running the Session Directory Service. [Ref. 44]

For the Windows Server 2003 computer, Session Directory must be visible on the network that is running the Terminal Services Session Directory service. Lastly, to be optimal, the Session Directory server needs to be a highly available network server that is not running Terminal Services.

g. Windows System Resource Manager (WSRM)

Microsoft Windows System Resource Manager is featured both in Windows Server 2003 Enterprise and Datacenter editions. WSRM provides the systems administrator the capabilities to manage and to allocate resources that include processors and memory resources. This feature decides among the multiple applications as to how the resources are allocated or managed based on the organization's business priorities. Essentially, the administrator sets guidelines for the hardware resources that an application or user is allowed to utilize.

Listed below are other capabilities incorporated in Windows System Resource Manager that provide the systems administrator with more functions to manage system resources:

- Set CPU and memory allocation policies on applications that includes selecting processes to be managed, and setting resource usage targets or limits.
- Manage CPU utilization in regards to percent CPU in use.
- Limit the process working set size such as the physical resident pages in use.
- Manage committed memory such as the page file usage.
- Apply policies to users or groups on a Terminal Services application server.
- Apply policies on a date or time schedule.
- Generate, store, view, and export resource utilization accounting records for management, service level agreement tracking, and charge-back purposes. [Ref. 45]

There are two different interfaces to administer WSRM. The graphical user interface provided by an administrative snap-in, and the command-line interface utilizes command-line scripting and supports advanced uses. Both user interfaces give the systems administrator access to the full functionality of WSRM.

Windows System Resource Manager is a useful tool that gives administrators the power to consolidate servers. The systems administrator can utilize reports that generate memory usage and CPU time to support service level agreement metrics. But most of all, WSRM provides more granularity and control of resources.

3. Windows Server 2003 Datacenter Edition

Windows Server 2003 Datacenter edition, built for the highest levels of scalability and reliability, is the most powerful and functional server operating system Microsoft has ever offered. This Windows family edition provides support to IT solutions that are required from databases, such as: enterprise resource planning software; high volume, real-time transaction processing; and server consolidation. Windows Server 2003 Datacenter operates in both 32-bit and 64 bit systems through specified original equipment manufacturer (OEM) partners who have qualify their company's hardware and software with Microsoft's Windows Hardware Quality Labs (WHQL).

WHQL ensures that OEMs produce quality hardware and software that interact efficiently and optimally with Microsoft's operating system, products, and technologies. As mentioned earlier, OEM products must qualify by passing the appropriate hardware compatibility tests conducted by WHQL. After successfully passing, the hardware product will be listed in an Enterprise Catalog and receive the certificate logo of "Designed for Windows." [Ref. 46] Microsoft's Web site (http://www.microsoft.com/windows/catalog/server/default.aspx?) Windows Server Catalog shows products and software compatibility tested for Windows Server 2003.

Other key features in the Datacenter edition are expanded physical memory space, Intel Hyper-Threading support, and direct access for storage area networks (SAN) with Windows Sockets. Feature highlights such as NUMA support, Cluster service, Terminal Services Session Directory, Windows System Resource Manager are included in Windows Server 2003 Datacenter and were already discussed in detail in the previous section, Windows Server 2003 Enterprise edition.

a. Expanded Physical Memory Space

Expanded Physical Memory Space provides Windows Server 2003, Datacenter edition, the capability to support Physical Address Extension (PAE) that operates on 32-bit Intel platforms. This feature allows administrators to extend the

system's memory to 64 gigabytes (GB) of physical Random Access Memory (RAM). In order to obtain peak performance and high quality of system with more than 4 GB of RAM, Microsoft has established a special Memory Support hardware compatibility list that provides a list of systems, devices, and drivers which have pass a test with this particular capability.

Windows Server 2003 Enterprise and Datacenter edition have PAE not enabled by default for systems that can support more than 4 GB of RAM. These operating systems are booted by default in normal mode which support only 4 GB of RAM. The /PAE switch must be added to the corresponding entry in the Boot.ini file in order to boot the system and utilize PAE memory. In addition, the system in the PAE mode needs an Intel Architecture processor that is a Pentium Pro or later model, more than 4 GB of RAM, and the Enterprise or Datacenter edition. [Ref. 47]

There are system board issues for platforms trying to support PAE. Such as the 64-bit platform, all peripheral component interconnect (PCI) adapters (this includes the 32-bit PCI adapter) need to be able to address the full physical address space in order to operate at the optimal performance. This issue requires a 32-bit PCI adapter to be able to support the Dual Address Cycle (DAC) command to all the transfer of 64-bit addresses to the adapter. If adapters cannot provide support for DAC, the PCI adapters will be unable to directly access the full address space on a 64-bit platform [Ref. 47].

b. Intel Hyper-Threading Support

Intel's Hyper-Threading Technology gives a single physical processor the ability to execute instruction streams, multiple threads, simultaneously which produces greater throughput and improves performance. Hyper-Threading Technology is currently being used in the Intel Xeon processor family for servers. Using these processors that contain two architectural states on a single processor, Windows Server 2003 Datacenter will view each physical processor to have two logical processors. With two logical processors, both processors will share the same execution resources of the processor core, and, unfortunately, the performance gains do not equate to having two complete physical processors [Ref. 48].

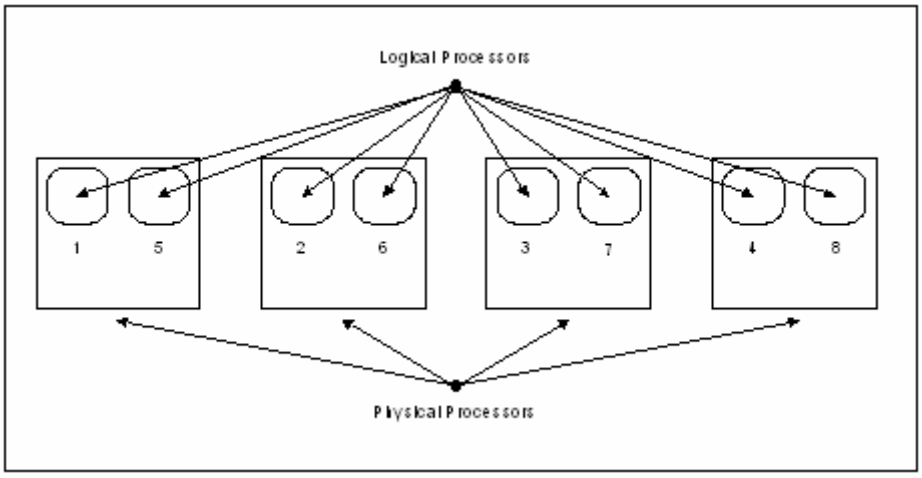

Figure 11. Example of a Four-Way System Enabled with Hyper-Threading Technology. (From Ref. [48].)

Windows Server 2003 Datacenter recognizes processors with Hyper-Thread Technology by receiving processor information from the BIOS. Intel provides and allows each server vendor to create its own BIOS. Having a system BIOS with Intel specifications, the operating system is permitted to recognize the BIOS by counting processors that use the first logical processor on each physical processor. Then, once Windows Server 2003 has counted a logical processor on all of the physical processors, the operating system will start counting the second logical processor on each physical processor. This counting process will continue as illustrated in the Figure 11 above. It is important that the BIOS count of logical processors is done as indicated in Figure 11. Otherwise, Windows Server 2003 or its applications will inadvertently use a logical processor when it should have used a physical processor.

As mentioned earlier, Hyper-Threading allows a system to execute more threads simultaneously per processor, which complements symmetric multi-processing. This process makes servers equipped with Intel Xeon take full advantage of logical processors created by Intel's Hyper-Threading Technology.

c. Direct Access for System Area Networks (SAN) with Windows Sockets

Windows Server 2003 Datacenter edition leverages System Area Networks architecture that allows the operating system to have direct access to SANs by utilizing Windows Sockets. System Area Network is considered to be a high-performing

and connection-oriented network that is able to link a cluster of computers. Surprisingly, SAN can deliver high bandwidths of 1 giga bit per second (Gbps) and with low latency [Ref. 49].

Compared to Ethernet and ATM network technologies used today, SAN provides a reliable transport service that delivers uncorrupted data in the same order in which the data was transmitted. In addition, SAN is not required to use the TCP/IP protocol stack unless it needs to transfer data that is routed between subnets. The bypassing of TCP/IP is achieved through the use of Windows Sockets. Windows Sockets provides increased speed and improved performance connection between two network nodes that are on the same system area network. This is achieved by mapping a SAN transport interface directly into an application process.

Through a SAN network interface controller (NIC) and a transport driver for the SAN NIC, the direct use of SANs is achieved by using the most of the network applications that are written to use TCP/IP protocol through Windows Sockets. In Figure 12, SAN architecture shows how Windows Sockets provides a SAN connection that allows Windows Server 2003 Datacenter to benefit from using SAN transparently without requiring modification.

As shown in Figure 12, the shaded area in the SAN architecture represents components that a SAN NIC vendor must supply to enable using SAN. The following briefly describes the components that are shown in the SAN architecture.

- **Windows Sockets Application** – Application that interfaces with Windows Sockets for network services.
- **Windows Sockets** – The Windows Sockets interface (Ws2_32.dll).
- **Windows Sockets SPI** – The Windows Socket service provider interface (SPI).
- **Windows Sockets Switch** – The Windows Socket switch switches between use of the standard TCP/IP service provider and particular SAN service providers.
- **TCP/IP** – A user mode DLL and associated kernel-mode proxy driver that comprise the standard base Windows Sockets service provider for TCP/IP. The proxy driver exposes a TDI (Transport Driver Interface) interface.
- **SAN Service Provider** - The user-mode DLL portion of the SAN service provider.

- **Proxy Driver for a SAN Service Provider** – The kernel-mode proxy driver of the SAN service provider.
- **NDIS Miniport Driver** – The NDIS (Network Device Interface Specifications) miniport driver that supports communication to the SAN NIC using the standard TCP/IP protocol driver.
- **SAN NIC** – The physical SAN network interface controller (NIC). [Ref. 49]

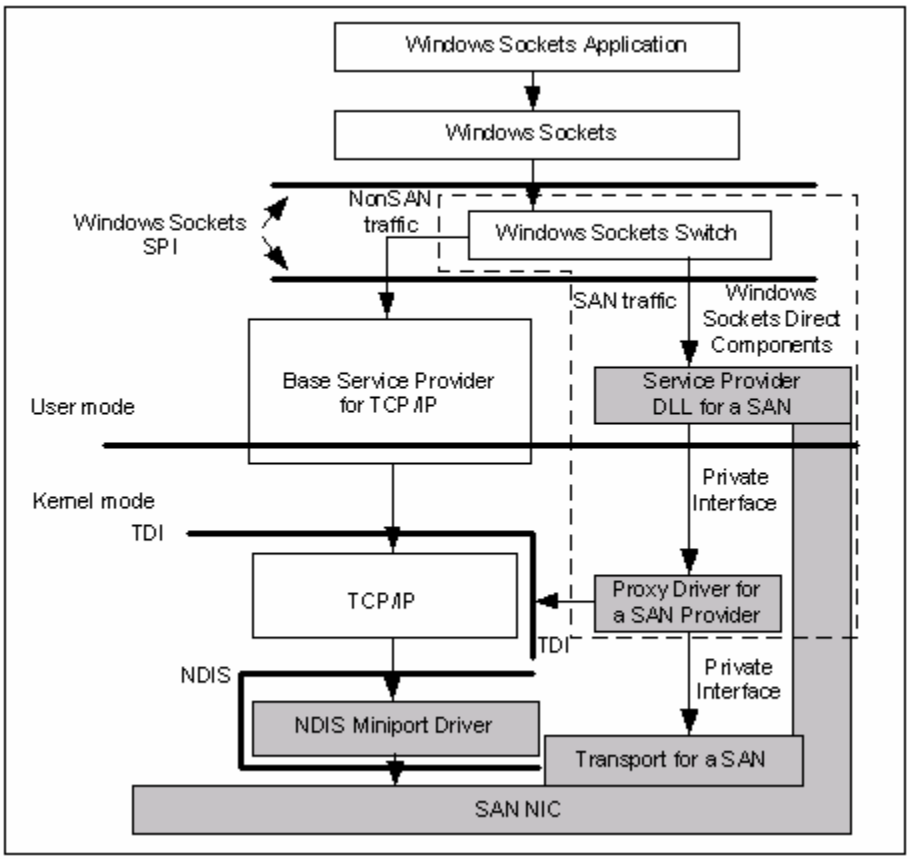

Figure 12. SAN architecture. (From Ref. [49].)

4. Windows Server 2003 Web Edition

Windows Server 2003 Web edition is dedicated to Web serving and hosting. This operating system delivers single-purpose solutions for Internet service providers, application developers, and other users who require the use or the need to deploy specific Web functionalities. Windows Server 2003 takes advantage of the improvements made with Internet Information Service (IIS) 6.0, Microsoft ASP.NET, and the Microsoft .NET

Framework in order to make it more simple to build and host Web applications, Web pages, and XML Web services. In this section, these features will be discussed later in more detail.

From Appendix A under the Hardware Specifications table, the table shows Windows Server 2003 supporting two-symmetric multiprocessing and 2 gigabytes of RAM. To reiterate, these two features allows applications to use multiple processors when additional processing power is needed. This is an important feature at providing a robust Web server.

a. Internet Information Service (IIS) 6.0

Internet Information Services 6.0 is included in all Windows Server 2003 family editions. IIS 6.0 is a Web server that enables an organization to easily deploy Web sites and provides a high-performance platform for applications designed to use Microsoft ASP.NET and Microsoft .NET Framework. The new redesign of IIS has improved security, increased Web server reliability and availability, and improved server management. The security improvements of IIS have been discussed in the previous chapter, and therefore will not be expounded upon in this section.

(1) Web Server Reliability and Availability - Web server reliability and availability in Internet Information Services 6.0 has increased due to features such as: the new fault-tolerant process architecture, health monitoring, automatic process recycling, and rapid-fall protection. The new fault-tolerant process architecture creates a self-contained unit called “application pools” that are used to isolate Web sites and applications. These application pools simply serve a set of Web sites and applications that increase reliability because the errors generated by one application will not cause another application pool to fail, or even worse cause the server to shut down.

IIS 6.0 has a feature called “health monitoring” that will periodically check the statefulness of an application pool and determine if any Web sites and applications with the pool have failed. If there is any occurrence of failures, an automatic restart on those failure Web sites and applications will occur which in turn increases application availability. In addition, health monitoring will automatically disable Web sites and applications that fail too often during a short amount of time. [Ref. 50]

Automatic process recycling is another feature in Internet Information Services 6.0 that automatically restarts and stops faulty Web sites and applications. While this feature queues requests, it uses a flexible set of criteria such as CPU utilization and memory consumption to determine when to restart and stop. Automatic process recycling also enables IIS 6.0 to maintain the client's TCP/IP connection when a worker process is being recycled (restart) and allows the Web services client applications to be isolated from back-end Web application instability.

Internet Information Services can protect Web servers against denial of service attacks by utilizing rapid-fail protection. This feature automatically disables an application that fails too often within a short amount of time. Then, IIS 6.0 will return a "503 Service Unavailable" error message to any new or queued requests to the application. Other actions such as debugging or administrator notification can be triggered as well.

(2) Improved Server Management - With Internet Information Services 6.0, an organization can manage a Web infrastructure with ease and more flexibility. The management tools in IIS 6.0 will reduce the amount of time systems administrators will take in managing Web server infrastructures. IIS 6.0 will provide easier management through new features such as XML-based configuration file, edit-while-running, command-line and script-based administration, and support for Windows Management Instrumentation (WMI).

XML-based configuration file, featured in IIS 6.0, uses XML-format and plain text meta-base, which is able to provide better means of executing backup and restore capabilities for servers that experience critical failures. From a management prospective, this tool enables IIS 6.0 in troubleshooting and meta-base corruption recovery. Also, IIS 6.0 can provide systems administrators an avenue to do direct editing by using common text editing tools.

Edit-while-running allows systems administrators to configure the Web server while it is operating. This feature in IIS 6.0 can be used to add a new Web site, add or create virtual directories, or change the configuration of application pools and worker processes; all of these tasks can be executed while IIS 6.0 continues to process

requests without any recompilation or restart. This tool decreases downtime of the Web server in respect to users and customers accessing the server.

With the Windows Server 2003 command-line, Internet Information Services 6.0 can accomplish common management tasks. This feature allows a single command to provide management of multiple local or remote computers. In addition, IIS 6.0 uses a complete scripting environment that automates common system administrative tasks by using the command-line without using the graphical user interface.

Windows Management Instrumentation (WMI) is fully supported by IIS 6.0. This feature provides Web administrators access to important management data that include performance counters and configuration files. The interfaces used with WMI are utilized to administer scripts and to make modifications on the XML-based configuration meta-base. [Ref. 50]

Internet Information Services 6.0 is a Web server that provides administrators more manageability in the organization's Web server infrastructure. With the features discussed above, Web serving is made easy to manage, and IIS 6.0 is an enabler that systems administrators can leverage when implementing Windows Server 2003.

b. ASP.NET

ASP.NET is the next version of Microsoft Active Server Pages. ASP.NET is more than the successor to ASP; it provides a unified Web development model that has available services pertinent to developers when building enterprise-class Web applications. ASP.NET is a compiled .NET-based environment that allows the administrators to author applications in any .NET compatible language, such as Visual Basic .NET, C#, and Jscript .NET. ASP.NET provides a variety of capabilities that are better than ASP, and some of these features that improve ASP.NET are listed below:

- **Page Framework** – A scalable programming model that allows the Web administrator to use on the server to dynamically generate Web pages.
- **Server Controls** – A set of controls that provide a structured programming model to access the properties, methods, and events of user interface controls for server-side code. With the use of Page Framework, Web administrator can create user controls and custom controls.

- **State Management** – Using HTTP, a stateless protocol, ASP.NET is able to maintain both application state and session state through the use of application and session variables.
- **Caching** – A general purpose cache facility for Web applications. It provides both a simple interface for caching and a more advanced interface that exposes expiration and change dependency services.
- **Data Binding** – Data binding allows Web administrators to bind components to data sources, including simple properties, collections, expressions, and methods that provide greater flexibility in using data from a database or other means.
- **Security** – ASP.NET provides Web administrators control to implement security by working in conjunction with IIS 6.0 security that includes the implementation of authentication and authorization services. In addition, ASP.NET uses a role-based security feature that can implement both Microsoft Windows and non-Windows user accounts.
- **Configuration** – Tasks including application settings such as database connections to security details and information about how errors should be handled are stored in files. These configuration files provide a location for computer-specific and application-specific information that can be changed without having to recompile the code.
- **HTPP Modules and HTTP Handlers** – An integral part of the ASP.NET architecture. Each ASP.NET request is processed by multiple HTTP modules and is then processed by a single HTTP handler. After the handler has processed the request, the request flows back through the HTTP modules. [Ref. 51]

Even an experienced Web administrator with ASP development skills will become very familiar to the new ASP.NET programming model. Of course there are differences. For example, the ASP.NET object oriented is more structured and object-oriented. Unfortunately, this makes ASP.NET not fully backwards compatible.

The features in ASP.NET allow Web administrators to connect users and customers to their organization's Web server. By accessing databases from ASP.NET applications, an often-used technique for displaying data to Web site visitors, ASP.NET has made it easier to access databases and to manage the database from the organization's code.

c. .NET Framework

In Windows Server 2003, the .NET Framework is an integral component in the operating system that allows administrator to build and run the next generation of

software applications and Web services. The .NET Framework is made up of the common language runtime and a unified set of class libraries. The common language runtime has many tasks. It is responsible for language integration, security enforcement, and memory, process, and thread management. For the set of class libraries, it provides standard functionalities that include input/output, string manipulation, security management, network communications, thread management, text management, and user interface design features. Supporting 20 different programming languages, the .NET Framework set of class libraries provides a common and consistent development interface across all languages supported by .NET Framework.

In addition to the common language runtime and class libraries, the .NET Framework has other new features, improvements to existing features, and enhancements to the documentation itself. Some of these features are native support for developing mobile Web applications, side-by-side execution, enable code access security for ASP.NET applications, and support Internet Protocol version 6 (IPv6). [Ref. 52]

(1) Native Support for Developing Mobile Web Applications - The .NET Framework features native support for developing mobile Web applications through ASP.NET mobile controls. The ASP.NET mobile controls utilize the ASP.NET server controls in order to adaptively communicate with the mobile device on the particular Web application which it is operating on. Using a browser detection, the mobile controls have adaptive capabilities to integrate with the individual devices ranging from full-featured personal digital assistant browsers to small, 5-line angstrom – 20 character mobile phone display [Ref. 52]. This adaptive feature allows the Web administrator to concentrate on Web applications as opposed to the device specific rendering decisions required from the mobile devices.

(2) Side-by-Side Execution - With the support of Side-by-Side execution, systems administrator can store and execute multiple versions of an application or component on the same computer. Side-by-Side execution does not mean that a managed application is compatible with other versions or components. But, this feature does allow the management of applications by choosing the components it executes with, and the multiple versions of the applications and components can coexist

on the same computer. To control this process, systems administrators can control the feature through the application's configuration file.

(3) Enable Code Access Security for ASP.NET Applications - Using code access security, systems administrator can further lock down the permissions granted to ASP.NET Web applications and Web services. Systems administrator can specify additional restrictions on selected application resources in the organization's policies. Obviously, these restrictions are in addition to a Windows Server 2003 system account that imposes security restrictions on applications. This feature can be applied to a shared server environment in order to isolate separate applications from one another, including stand alone servers that require applications running with the minimum amount of privileges.

(4) Support Internet Protocol Version 6 (IPv6) - .NET Framework supports Internet Protocol Version 6, which is a new suite of standard protocols for the network layer of the Internet. IPv6 was designed to resolve numerous issues of the current version of IPv4, such as address depletion, security, auto-configuration, and extensibility. Essentially, as the Internet grows exponentially and the number of addresses used on the Internet is increasingly getting larger, the support of IPV6 will significantly increase the address spaces that will be used for identifying communication endpoints on the Internet [Ref. 52].

IPv6 is in the process of being a standard protocol for the Internet. This new protocol was developed because of the increased use and development of Internet-connected devices and appliances that are depleting the address capacity of IPv4. [Ref. 53] The increase of addresses is just one of many features in IPv6; the features in the protocol are as follows:

- New header format
- Large address space
- Efficient and hierarchical addressing and routing infrastructure
- Stateless and stateful address configuration
- Built-in security
- Better support for Quality of Service

- New protocol for neighboring node interaction
- Extensibility [Ref. 53]

The features above will enable any organization to leverage new technological devices using IPv6. This protocol will make the Internet experience more robust through the numerous innovative advances in IT, particularly the Internet.

5. Windows Server 2003 Small Business Edition

Windows Server 2003 Small-Business edition is comprised of several Microsoft server products that a small organization, particularly a business type, can leverage in order to share information and resources in a safe and secure network environment. The Small Business edition's integration of the numerous server products provides features that are included in Windows Server 2003 Standard edition, and more. There are two different editions of Windows Server 2003 Small-Business, Standard and Premium.

Standard edition features the following Microsoft products:

- Windows Server 2003 Standard edition – provides an enhanced security, reliable operating system that keeps data available on the network, Active Directory directory services and tools.
- Windows SharePoint Services – Provides team communication and collaboration environment.
- Exchanger Server 2003 technology – Provides communication, messaging and collaboration infrastructure; Microsoft Outlook Web Access to enable email access via the Web.
- Microsoft Office Outlook 2003 – Provides a central place to manage email, calendars, contacts, and other personal and team information.
- Microsoft Shared Fax Service – Provides fax with fewer telephone lines by utilizing users' desktops and allowing users to set hours; receives faxes through SharePoint, e-mail, or printer.
- Routing and Remote Access Services – Provides a firewall technology to secure Internet connections. [Ref. 9]

Premium edition has all the features in Standard with three additional products:

- ISA Server 2000 technology – Provides firewall technology to secure Internet connections.
- SQL Server 2000 – Provides relational database that supports line-of-business applications.
- Microsoft Office FrontPage 2003 – Provides tools to create and develop sophisticated Web sites for Windows SharePoint Services. [Ref. 9]

The Standard and Premium edition of Windows Server 2003 Small-Business is a business server solution that a small organization can deploy to improve the organization's IT infrastructure. This family edition of Windows Server 2003 will allow small businesses to do more with less.

B. WINDOWS SERVER 2003 FEATURES

Windows Server 2003 is more than just an operating system, but a new innovative server that uses technological advances in order to provide systems administrators the tools to effectively deploy and manage an IT infrastructure. In this section, several feature highlights in the operating system will be discussed. These features are mainly in the realm of server roles such as, file and print server, Web server, Mail server, and Terminal server, some of which have already been discussed in earlier chapters and sections.

The diverse set of server roles listed can be handled by Windows Server 2003 because of the different services that the operating system is capable of deploying. Services provided in Windows Server 2003 will be discussed and are listed in the following: Directory Services, Security Services, Terminal Services, Interoperability Tools, Communications and Networking Services, File and Print Services, Management Services, .NET Application Services, and Multimedia Services.

1. Directory Services

Directory Services provides a repository for information about network-based entities or objects, such as applications, files, printers, and people. This feature gives systems administrators the capability to consistently name, describe, locate, access, manage, and secure information about these different resources. Two features that can be used for Directory Services are Active Directory and Meta-Directory Services Support. Meta-Directory Services Support, centrally stored and integrated identity information from multiple directories, was discussed earlier. Therefore, this section will focus on the improved features in Active Directory that include the following: Active Directory Migration Tool version 2.0, Domain Rename, Schema Redefine, Active Directory in Application Mode, Group Policy Improvements, and Enhanced User Interface.

a. Active Directory Migration Tool Version 2.0 (ADMT)

Most systems administrators will develop a strategy to upgrade from an existing operating system to the most current one. This migration process is very tedious, and by using Active Directory Migration Tool, it will provide an easier means of migrating from Microsoft Windows NT 4.0 to Windows 2000 and Windows Server 2003 or from Windows 2000 to Windows Server 2003 domains. The command line interface utilized in ADMT 2.0 simplifies the process. In addition, most migration tools cannot copy passwords; Windows Server 2003 includes an ADMT, but it is really intended for small scale migrations of a thousand users at the most [Ref. 1].

There are two types of migration to an Active Directory (AD): "in place" upgrades and "clean and pristine." In place upgrades allow Windows Server 2003 to convert the domain from its current SAM file (NT4), or Active Directory (Windows 2000) to a Server 2003 based AD. For the clean and pristine migration, this approach leaves the current domains, whether NT 4, Windows 2000, or 2003 based AD domains, alone and create a new, empty AD domain. Both migration approaches have its advantage and disadvantage that are listed below in Table 3.

Table 3. Advantages and Disadvantages of "In Place Upgrades" and "Clean and Pristine" Migration Approaches. (After Ref. [1].)

	ADVANTAGES	**DISADVANTAGES**
In Place Upgrades	▪ Do not require new machines. ▪ Users keep old SIDs and the domain keeps its old trust relationships. ▪ Users keep old passwords. ▪ Simple and quick upgrade. ▪ Going from 2000 based AD to 2003 based AD seems more of a trouble-free process.	▪ Cannot make former NT primary domain controllers (PDC) into a domain controller on an existing AD domain; upgrading a PDC will always result in the creation of a new AD domain. ▪ Cannot set the new domain's NetBIOS name, as it's automatically set equal to the old NT 4 domain's name. ▪ Cannot merge old NT 4 domain into an existing AD domain. ▪ Upgrading all of the accounts is a one-way trip; there is no AD Rollback Wizard. ▪ Any leftover junk in the old NT 4 Domain SAM remains in the new AD database.

Clean and Pristine Migration	▪ Allows a systems administrator to do gradual upgrades. ▪ Copies user accounts and doesn't move them. The old accounts are still there if something goes wrong. ▪ Lets administrator create Domain Controllers from clean installs, avoiding the extra complexity and potential bugs of an in-place upgrade. ▪ Allows systems administrator to consolidate domains, collapsing a quagmire of many domains into just one, or just a few.	▪ Needs more machines than when/if upgrading because the new machines will be needed to act as domain controllers in the new domain. ▪ Most migration tools cannot copy passwords. The users will have to create new passwords the first time logging in to the new AD domain. ▪ Need to purchase a migration tool capable of migrating more than 1,000 user accounts. ▪ Cannot create an AD domain with the same NetBIOS name as the old NT 4 domain because that would require the administrator to create two domains with the same NetBIOS name. ▪ Requires more work. Administrators will need to know when to move any given set of users.

b. Domain Rename

Domain Rename, supported by all Windows Server 2003 operating systems except Web edition, is a feature that processes the change of the names of domains and the change of the structure of the domain trees in a forest. These processes are done by updating the Domain Name System and the trust infrastructures, which include the Group Policy and service principal names. Essentially, Domain Rename allows the systems administrator to make important name changes and forest structural changes as required because of various organizational changes.

The domain rename process can be applied to different scenarios such as acquisitions, mergers, or name changes in the organization, but it will not allow for forest mergers or the movement of domains between forests. More importantly, domain rename in Windows Server was designed to be a supportive method for renaming domains when domain renames are required. It is not intended to be utilized in making domain rename a routine operation. The systems administrator needs to realize that the domain rename process is somewhat complex and requires a lot of forethought in the planning and

execution. In addition, the amount of time required to process and complete a domain rename will be dependent upon the size of the Active Directory forest, especially the number of domains, domain controllers, and member computers.

Although Windows Server 2003 forest has domain rename and restructuring capabilities, the systems administrator should know some features that are not supported by the Domain Rename process. The domain rename process is not a trivial operation and therefore the systems administrator should consider the following things that Windows Server 2003 forest cannot do when executing a domain rename and restructuring.

- Cannot change which domain is the forest root domain. Changing the DNS name or the NetBIOS name or both of the forest root domain is supported.
- Cannot drop domains from the forest or add domains to the forest. The numbers of domains in the forest before and after the domain rename and restructuring operation need to remain the same.
- Cannot rename a domain with a name that was taken from another domain in a single domain rename and restructuring operation. [Ref. 54]

Even though there are features that Domain Rename cannot support, it is a useful tool that allows the systems administrator to change the structure of the domain hierarchy when a parent of a domain needs to be changed or a domain residing in one domain tree requires to be moved to another domain tree. Listed below are several kinds of changes that the Domain Rename process is capable of executing in a Windows Server 2003 forest.

- Simple renaming without repositioning any domains in the forest structure.
- Creating a new domain tree structure by repositioning domains within a tree.
- Creating new trees. [Ref. 55]

To re-emphasize to systems administrators: exercise extreme caution when executing the Domain Rename tool because it is not a simple task; it is very complex. Microsoft has hundreds of pages online documenting its tedious process, and these documents should be read thoroughly before trying the process on a real domain. [Ref. 1]

c. Schema Redefine

Schema Redefine provides Windows Server 2003 Active Directory (AD) the ability to deactivate attributes and class definitions in the AD schema. The schema consists of object definitions and is the AD component defining all the objects and attributes used by the directory service to store data. Since the schema dictates how information is stored, systems administrators need to tightly control the process because any schema changes can affect every domain controller. The schema should be tested to ensure there are no adverse affects on the rest of the forest.

Schema has three basic components called objects, attributes, and classes. Objects are structures that store both data that the objects represent and data that controls the content and structure of the objects. Attributes contain data that define the information stored in an object or in another attribute. Classes categorize object definitions into groups and acts like a blueprint that can be used each time a new object is created. Schema object are the attributes and classes in AD that are stored in the schema partition as directory objects.

The information in the schema can be removed through the process of deactivation. This process can render the object definition unusable and can no longer be used to create new objects in the directory. Any object definition deactivated is referred to as defunct. When deactivating existing classes and attributes, the deactivation of these schema classes and attributes is subject to the restrictions listed below:

- Cannot deactivate a class or attribute that appears in the base AD schema. Systems administrators can only deactivate schema extensions of the base schema.
- Cannot deactivate an attribute that is referenced in the *mustContain*, *ssytemMustContain*, *mayContain*, s*ystemMayContain*, or *rdnAttId* properties of an active class.
- Cannot deactivate an attribute that is referenced in the *subClassOf*, *auxiliary Class*, or *possibleSuperior* properties of an active class. [Ref. 56]

In order to deactivate an attribute, the *isDefunct* attribute is set so that its *attributeSchema* object is TRUE. By setting *isDefunct* to TRUE, the attribute can no longer be added to new class definitions. Setting the *isDefunct* attribute to FALSE, the attribute is reactivated. To deactivate a class, the *isDefunct* attribute must be set so that its

classSchema object is TRUE. This setting will no longer allow the creation of new object instances of the class. Setting the *isDefunct* attribute to FALSE will reactivate the class.

d. Active Directory in Application Mode (AD/AM)

Active Directory in Application Mode is a new feature in Windows Server 2003 Active Directory. This feature provides data storage and retrieval for directory-enabled applications that are not dependent on the Active Directory Services schema extensions. Most directory-enabled applications require the directory service to have application–specific schema extensions. AD/AM is a new mode of AD that is designed to allow organizations to support these directory-enabled applications by providing much of the same functionalities, such as multi-master replication, as AD, without the need of deploying domains or domain controllers.

Using Active Directory in Application Mode, systems administrators can run multiple instances of AD/AM at the same time on a single computer that uses an independently managed schema for each AD/AM instance. Figure 13 illustrates an AD/AM configuration that has a computer running AD/AM and is hosting three separate AD/AM instances. Each AD/AM instance is using an independently managed schema and data, and supports a different directory-enable application. In addition, each computer can reside within or outside the AD forest.

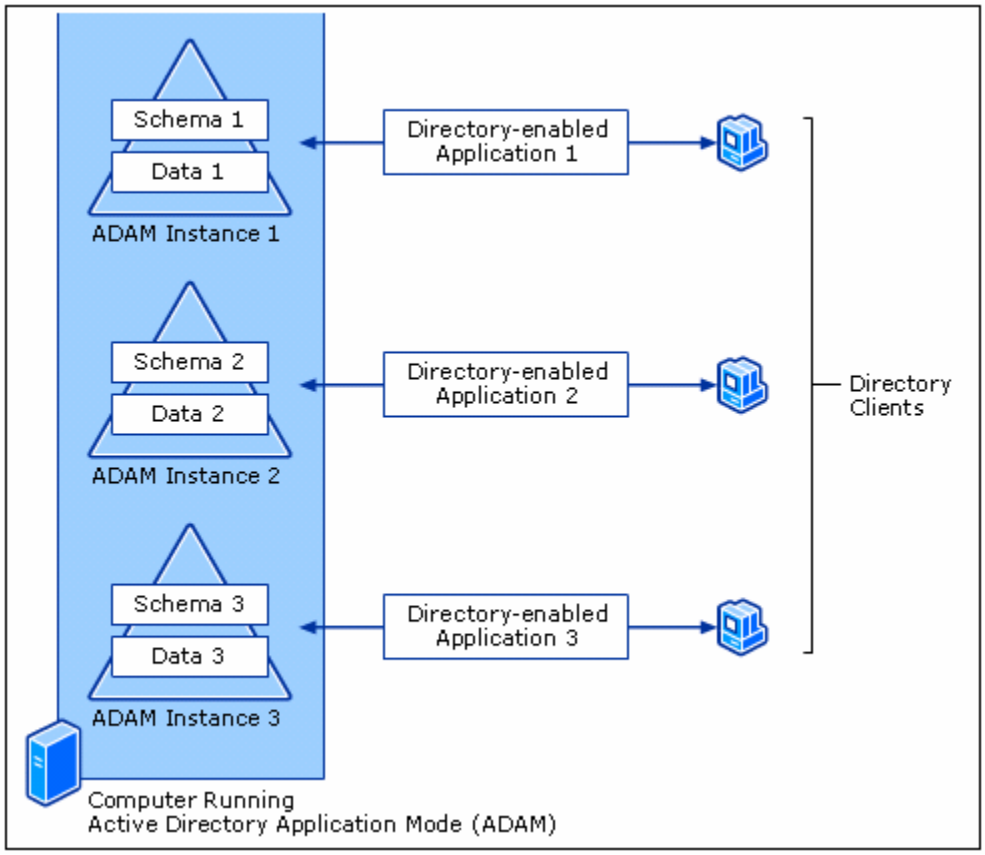

Figure 13. An Example of an AD/AM Configuration. (From Ref. [57].)

Based on the same source code as Active Directory, AD/AM is a special mode of AD, and to some extent, it operates very similarly to AD. There are some differences because AD/AM was designed mainly to support directory-enabled applications without the reliance of network operating system operations. As shown in Figure 13, each computer is running an instance of AD/AM rather than the system service. Some of the differences between AD/AM and Active Directory are the following:

- Supported operating systems
- Schema
- Partition naming
- Directory instance management
- Replication
- Dependencies

- Performance and scalability [Ref. 57]

To compare the two further, the table below shows a list of operating systems that are supported by AD and by AD/AM.

Table 4. Operating Systems Supported by Active Directory and AD/AM. (After Ref. [57].)

Directory Service	Platforms Supported
Active Directory	• Domain controllers running Microsoft Windows 2000 Server • Domain Controllers running Windows 2000 Advance Server • Domain controllers running Windows 2000 Datacenter Server • Domain controllers running Microsoft Windows Server 2003, Standard Edition • Domain controllers running Microsoft Windows Server 2003, Enterprise Edition • Domain controllers running Microsoft Windows Server 2003, Datacenter Edition
Active Directory in Application Mode	• Computers running Windows XP Professional • Domain controllers and servers running Windows Server 2003, Standard Edition • Domain controllers and servers running Windows Server 2003, Enterprise Edition • Domain controllers and servers running Windows Server 2003, Datacenter Edition

Again, schemas provide definitions for what kind of information a directory can hold. There are differences with AD and AD/AM in the uses of schemas. In an Active Directory, a single schema will be applied to an entire forest that requires all domain controllers to use the same schema. In contrast, every stand-alone AD/AM instance or AD/AM configuration set can have its own schema that is fully independent from the Active Directory schema. Running these multiple instances of AD/AM on a single computer will allow an organization to consolidate directory operations on a single server or just a few servers. The size of the base schema is another difference between

AD and AD/AM. Since the base schema of Active Directory is designed to support the network operating system operations, it is considerably larger. On the other hand, the base schema of AD/AM is much smaller because it is only large enough to bootstrap the AD/AM instance and because it was specially designed to use the extensions of schema elements that are required by applications using AD/AM instances. Lastly, any object class in AD/AM can be utilized to authenticate against or bind to the directory by adding the *msDS-bindableobject* auxiliary class and the *unicodePwd* attribute to the schema definition of an object class. In contrast, the Active Directory can only have certain object classes that can be used to bind or authenticate against the directory.

The naming of partitions is somewhat different in AD and AD/AM. The logical portion of the directory data store is the directory partition. For each AD/AM directory partition, each has its own unique distinguished name. The naming process for an AD/AM partition is more flexible than for an Active Directory. The AD supports only Domain Name System (DNS) style names for top-level directory partitions, and such names can contain only the "DC=" naming components. For example, the Active Directory of an organization might have a partition named DC=NPS, DC=COM, but the directory partition cannot have a partition named DC=NPS, C=US. In AD/AM, it supports both the DNS style and the X.500 style names for top-level directory partitions. Listed below are all the distinguished name components that are supported by AD/AM.

Table 5. AD/AM Directory Partition Distinguished Name Components. (After Ref. [57].)

Distinguished Name Component	Description
C=	Country/region
CN=	Common name
DC=	Domain component
L=	Location
O=	Organization
OU=	Organization unit

From the above table, AD/AM can have a directory partition named DC=NPS and C=US, which is different from the AD partitioned naming that is limited to using only DNS style.

In regards to server consolidation, Active Directory is unable to consolidate because of the limitations that are applied on the AD by forests and domains that require each domain controller to run only one instance of AD. On the other hand, AD/AM can run multiple directory service instances on each computer. As mentioned earlier, this process consolidates the directory operation on a single server or just a few servers by running on multiple instances of AD/AM.

The replication process for an AD requires its domain controllers to replicate with each other, which is based on memberships in a domain. AD/AM instances replicate with each other through a process that is based on memberships in a configuration set. This configuration set is a group of AD/AM instances that share and replicate a common configuration partition and schema partition. The process for an AD/AM does not allow replicating with AD. In addition, AD/AM instances replicate on a schedule that is completely independent of the AD replication schedule, even if AD/AM is running in an AD. [Ref. 57]

A major difference between AD/AM and AD is how dependent AD requirements are. For example, AD requires or relies on forests or domains while

AD/AM does not. Also, AD/AM does not rely on File Replication service or DNS, and both services are required in order for AD to operate properly.

Lastly, AD/AM is able to support similar number of users, sites, and objects as Active Directory. This shows that AD/AM is comparable to AD because both are based on the same code, and both are equal in scalability and in performance characteristics.

e. Group Policy Improvements

Windows Server 2003 has improved its Group Policy features with its new Group Policy Management Console (GPMC). This new tool of Group Policy provides a unified graphical user interface (GUI) that deploys and manages Group Policy implementations and enables script-based management of Group Policy operations. GPMC allows systems administrators to manage multiple domains and sites within a given forest, as mentioned earlier, with a simplified GUI that uses drag-and-drop support. GPMC is the central place for managing many aspects of Group Policy, and GPMC provides the following functionalities:

- Backup/restore of Group Policy objects (GPOs).
- Import/export and copy/paste of GPOs and Windows Management Instrumentation (WMI) filters.
- Simplified way of managing Group Policy-related security.
- HTML reporting of GPO settings and Resultant Set of Policy (RSoP) data.
- Scripting of policy- related tasks. [Ref. 58]

The functionalities above are fully scriptable and allow the systems administrators to easily customize and automate the management of Group Policy.

Group Policy operations such as backup, restore, import, and copy GPOs are tasks used to manage Group Policy. Backing up a GPO entails the making of a copy of GPO data to the file systems. Restoring a GPO requires the backup of an existing GPO and re-instantiating it back in the domain. The purpose of this is to reset a specific GPO to its identical state before it was backed up. Importing a GPO enables a systems administrator to transfer settings from a backed up GPO to an existing GPO, whether the GPO is in the same domain, across domains, or across forests. Restoring and importing a

GPO removes any existing settings already in the GPO. Only the settings in the backup will remain when this operation is completed. Lastly, copying a GPO is like exporting/importing except that the GPO is not saved to a file system.

Backup operation allows the systems administrator to only back up components of a GPO that are in the GPO in Active Directory and in the GPO file structure. This operation does not copy items stored outside the GPO, like the WMI filter and IP Security policies.

Restore operation restores a GPO to a previous state. This operation is used to restore because the GPO may have been backed up but it was later deleted or the GPO is live and the systems administrator wants to roll back to a known previous state. In addition, the restore operation does not restore links to a Scope of Management.

Import operation transfers settings to an existing GPO in Active Directory by using a backed up GPO in the file system location as its source. This operation can be used transferring settings across GPOs within the same domain, a cross-domain in the same forest, or a cross forest. Import operation can be used for migrating Group Policy across environments where there is no trust.

Copy operation transfers settings by using an existing GPO in Active Directory as the source and creates a new GPO as its destination. This operation transfers the settings to a new GPO either in the same domain, a cross-domain in the same forest, or a cross forest. Unlike the import operation, trust is required between the source and the destination domains or the systems administrator must gain access to the untrusted forest by using the Stored User Names and Passwords tool.

Windows Management Instrumentations Filters is a new feature in Windows Server 2003 that enables the systems administrator to determine the scope of GPOs based on attributes of the target computer. As a separate object, the WMI filter can link to a GPO, and when the GPO is applied to the target computer, the filter is evaluated on the target computer. This process has the WMI filter, consisting of one or more queries, evaluated against the WMI repository of the target computer. If the evaluated filter is false, the GPO is not applied. But, if the all the queries evaluate to true, the GPO is applied. Systems administrators must note that client support for WMI filters exist

only on Windows XP and later operating systems. Also, each GPO can have only one WMI filter, but, the same WMI filter can be linked to multiple GPOs. Like GPOs, the WMI filters are per domain objects. [Ref. 58]

Group Policy Modeling, a new feature in Windows Server 2003 Group Policy Management Console, allows the systems administrator to simulate a policy deployment in order to apply it to users and computers before actually implementing the policy. This integration feature is also known as the Resultant Set of Policy (RSoP) and is a Planning Mode in Windows Server 2003. These simulations can only be performed by the services that are present only in Windows Server 2003 domain controllers. But, the feature can simulate the RSoP for any computer in the forest that can include those running Windows 2000.

Similar to the data in Group Policy Modeling, Group Policy Results is a feature that enables systems administrators to determine the resultant set of policy that was applied to a given computer and user logging on to that particular computer. The data are determined by actual results from the client, a contrast to the Group Policy Modeling, which determines its data through simulations on the domain controller. This feature requires its clients to be running Windows XP, Windows Server 2003, or later because it is not possible to get Group Policy Results data for a Windows 2000 computer.

Scripting Group Policy-related tasks can be accomplished through GPMC's user interface. This user interface is based on a set COM interfaces that are available to Windows scripting technologies such as Jscript and VBScript, other programming languages like Visual Basic, and VC++. With the user interfaces, the following capabilities are scriptable:

- Creating/deleting/renaming GPOs.
- Linking/unlinking GPOs and WMI filters.
- Delegation.
- Security on GPOs and WMI filters.
- Group Policy-related security on sites, domains, OUs.
- Creation rights for GPOs and WMI filters.
- Generating reports of GPO settings.

- Generating reports of RSoP data.
- Backup/Restore of GPOs.
- Import/Export, Copy/Paste of GPOs
- Search for GPOs, WMI filters, Scope of Management, and backups. [Ref. 58]

Table 17 of Appendix B shows a list of scripts to do the associated types of Group Policy administrative tasks. Using a number of the sample scripts that are written mostly in VBScript, the systems administrator can form a toolkit of scripts to directly administer a Group Policy environment. In addition, these scripts can be used to build more elaborate management tools.

f. Enhanced User Interface (UI)

Enhanced User Interface is the key features of Windows Server 2003. UI has been the principal means in managing enterprise identities, objects, and relationships. This feature has increased the systems administrator's ability to integrate capabilities through Microsoft Management Console plug-ins. These plug-ins have included the following capabilities: drag-and-drop capabilities, multi-object selection, and the ability to save and reuse queries. With some of these plug-ins, systems administrators can edit multiple user objects simultaneously, can reset access control list permissions to the default, show effective permissions on a security principal, and indicate the parent of an inherited permission. User Interfaces are a management tool that is utilized by Windows Server 2003 to provide the systems administrator the most efficient manner in managing the network system.

2. Security Services

Security was the main focus of this thesis. The Security Services in Windows Server 2003 was highlighted in the previous chapter that covered many aspects of the enhanced features and new improvement in regards to security. To reiterate, the chapter discussed topics ranging from the Internet Connection Firewall to the Public Key Infrastructure features introduced in the new operating system. Chapter II can be revisited and reviewd for more details.

3. Terminal Services

Terminal Services in Windows Server 2003 allows systems administrators to deliver Windows-based applications, or the Windows desktop, or virtually any computing

device, even those that cannot run on Windows. This feature runs applications on the Terminal Server, and the application executes on the server, and only the keyboard, mouse, and display information is transmitted over the network. This process is independent from any other client session and is managed transparently by the server operating system, which allows each user to see only his or her individual session.

The highlighted features in Terminal Services are Remote Desktop for Administration and Terminal Server Session Directory. Terminal Server Session Directory has been discussed in the previous section, and therefore the focus here will be Remote Desktop Administration. Terminal Services has several new features that are incorporated in the Remote Desktop for Administration, and these improvements include: Remote Desktop Connection, Improved Client Interface, and Client Resource Redirection.

Remote Desktop for Administration is a feature that provides remote management of Windows Server 2003 servers. Utilizing this feature, the systems administrator and operators can remotely access back-end servers and domain controllers by means of a graphical user interface-based tools available in the Windows environment, and, as mentioned earlier, the administrator does not have to use a Windows-based computer to administer the server. Remote Desktop for Administration has the following capabilities:

- Graphical administration of Windows Server 2003 and Windows servers from any Terminal Services client.
- Remote upgrades, reboots, and promotion and demotion of domain controllers.
- Access to servers over low-bandwidth connections, with up to 128-bit encryption.
- Roaming disconnect support: this feature enables data-sensitive or time-consuming tasks to be completed successfully if the remote session is disconnected deliberately, or due to network problems.
- Remote application installation and execution, and with fast access to local disks and media.
- Negligible performance impact on the server and no impact on application compatibility.
- Two remote administrators can share a session for collaboration purposes.

- Remote Desktop Protocol (RDP) feature set includes local and network printing; file system redirection; clipboard mapping; smart card redirection; serial device redirection; and support for any RDP virtual; channel applications. [Ref. 59]

Remote Desktop Connection (RDC) is the new Terminal Services client that leverages the latest Microsoft Remote Desktop Protocol (RDP) 5.2 version. This protocol allows communication over TCP/IP network connections, is tuned for high and low bandwidth environments, and supports three levels of encryption. The connection for RDC has been improved by fully integrating Connection Manager into RDC. This improvement has allowed users and administrators to save connection settings files and use them locally or deploy them to other users. Saved passwords that are encrypted can only be decrypted from the original computer. In addition, RDC can support automatic restoration of interrupted network connections if a connection is dropped while the systems administrator is in the middle of a process. With RDC, the connection will be reconnected to the session without losing the administrator's place, essential when processing critical mission tasks.

The Remote Desktop Connection client interface has been improved with a full-screen and high-color session. The connection bar allows quick switching between the remote session and the local desktop. In addition, the interface can be customized to suit the administrator's needs, such as options for display, local resources, programs, and experience. The experience setting allows the administrator to select the connection speed and graphic options, like themes or menu and Windows animation, in order to optimize performance of the system for lower bandwidth connections.

Remote Desktop Connection supports a wide variety of data redirection types that are available to clients on Windows Server 2003 or Windows XP Professional. To increase security, each type of redirection can be disabled by either the client or the server. In order to warn users, a security alert is displayed when the file system, port, or smart card redirection is requested, and then provides the user a means to refuse the redirection or to cancel the connection at that time. In Table 6 below, the new features in client resource redirection can be used by any computer that can run Remote Desktop Connection.

Table 6. Client Resource Redirection Features. (From Ref. [60].)

FEATURE	DESCRIPTION
File System	Client drives, including network drives, are mounted inside the server session. This lets users open or save files on their own computers' disk drives, in addition to opening and saving files on the server.
Ports	Client serial ports can be mounted to the server. This enables a variety of hardware on the client computer to be by software on the server.
Printers	All printers installed on the client are visible to the server—including network printers. With Windows 2000 Terminal Services, only locally-connected printers are redirected. Redirected printers are given names that are easier to read. For example, users might see: "printername on printserver (from clientname) in session 9"; whereas in Windows 2000, they would have seen "_printserver_printername/clientname/Session 9." Printer redirection also works when connecting to Windows 2000-based servers.
Audio	Sounds such as "error" and "new mail" notification events are redirected to the client.
Smart Card Sign On	A smart card containing Windows log-on credentials can provide those credentials to a Windows Server 2003 remote session for log-on. This feature requires a client OS that can recognize the smartcard first: Windows 2000, Windows XP, and Windows CE .NET.
Windows Keys	Keys such as **Alt-tab** and **Control-Escape** are sent to the remote session by default. The **Control-Alt-Del** combination is always interpreted at the client computer for security reasons. **Note** These redirections also work when connected to a Windows 2000-based terminal server, but only when using Windows NT-based client operating systems. They do not work with Windows 9x-based operating systems.
Time Zone	A RDC client computer can provide its time zone to the server, or users can manually set their own time zones. This enables an administrator to use one server for multiple users across different time zones. It's also helpful for applications that support features such as calendars. **Note** This feature is off by default, because it relies on a properly-set time zone on the client computer.
Virtual Channels	Virtual Channels can be used to move data between client and server computers. This feature is available in both Windows Server 2003 and Windows 2000 Server.

4. Service for UNIX (SFU)

Service for UNIX is a feature in Windows Server 2003 that provides full range support and integration between cross-platform network services that are geared toward interoperability among Windows and UNIX-based environments. This feature provides users and administrators access to information stored in multiple platforms and allows consolidation in the management of networks, and enables the reuse of UNIX applications and scripts on Windows. The latest Service for UNIX version is SFU 3.5. This version has significant new features and enhancements that demonstrate the big shift in how interoperability of scripts and programs are accomplished. SFU enhanced

features include Network File System (NFS) Support, Server for Network Information Systems and Password synchronization, Telnet, and Interix. The table below describes the new features in the Windows Server 2003 latest version of SFU.

Table 7. New and Enhanced Server for UNIX 3.5 Features. (From Ref. [61].)

FEATURE	DESCRIPTION
NFS Client	▪ Support setuid, setgid and sticky bits. ▪ Support for symbolic links. ▪ Performance improvements. ▪ Internationalization: additional language options.
NFS Server	▪ Significant performance enhancements. ▪ Support for active-active clustering of NFS shares. ▪ Support for setuid, setgid, and sticky bits. ▪ Per-share handing of root and anonymous access. ▪ Improved model for mapping permissions between Windows and UNIX. ▪ Internationalization improvements. ▪ Support for Windows Server 2003 Volume Shadow Copy Service. (SFU 3.5) ▪ Simplified and enhanced authentication in Windows Server 2003 Active Directory environments. (SFU 3.5)
NFS Gateway	Internationalization improvements.
Mapping Server	▪ Cluster-enabled mapping server. ▪ Performance, security, and scalability improvements. ▪ Support for redundant mapping servers. ▪ Internationalization improvements.
Server for NIS	▪ Support for MD5 encryption. ▪ Scalability and performance improvements. ▪ Numerous usability and administration improvements.
Password Synchronization	New support for setting passwords using Pluggable Authentication Model on UNIX.
Telnet Server	▪ IPv6 support. ▪ Internationalization improvements.
Interix and the Interix Software Development Kit	▪ All new to SFU 3. ▪ Improved throughput and stability. ▪ Single-rooted file system.

5. Communications and Networking Services

Communications and Networking Services for an organization have never been more critical in staying ahead of other organizations, especially with today's advances in IT. There are new networking features and improvements in Windows Server 2003 that have made computing versatile. Some features have already been discussed in the

previous chapters, such as IPv6, IAS/RADIUS, NLB, and Network Access Security with 802.1X. This section on Communication and Networking Services will focus on features in Virtual Private Network (VPN) Support, Network Bridge, and Internet Connection Sharing (ICS) [Ref. 62].

a. Virtual Private Network (VPN) Support

Virtual Private Network Support in Windows Server 2003 provides users access to an organization's network, even when the user is out of the office, by deploying a VPN. The VPN connection creates a medium that is a secure tunnel across the Internet into the private network. To be discussed later in this section, the VPN connection is created by using two types of technology in the Windows Server 2003 family: Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP). VPN technology allows organizations to connect branch offices or to other organizations via a public inter-network, such as the Internet. While maintaining a secure communication, the VPN connection across the Internet logically operates and appears to the user as a private network communication. This connection is communicated over the public inter-network, therefore, called virtual private network.

In Figure 14, a point-to-point link is emulated by having data encapsulated or wrapped with a header, which provides routing information that allows the data to traverse the shared or public transit inter-network in order to reach the other endpoint. In order to create a private link, the data being sent are encrypted for confidentiality. The encryption used allows packets to be indecipherable without the encryption keys, even if they are intercepted on the shared or public network. The connection part where the private data are encapsulated is called the tunnel, and the connection part where the private data are encrypted is called the VPN connection.

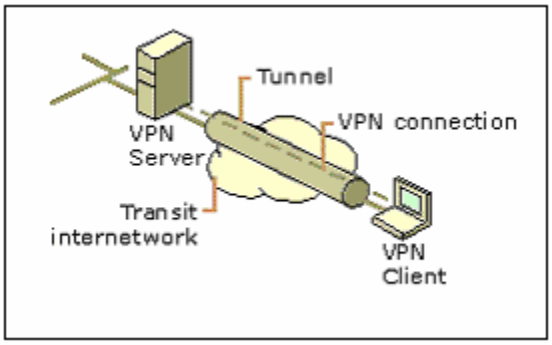

Figure 14. Virtual Private Network (VPN) Connection. (From Ref. [63].)

(1) Point-to-Point Tunneling Protocol (PPTP) - Point-to-Point Tunneling Protocol enables an organization to encrypt data that are of multi-protocol and afterwards encapsulates the data in an IP header to be sent across an organization's network or the public Internet. Using Point-to-Point Protocol (PPP) frames, PPTP encapsulates PPP frames in IP datagrams in order to transmit them over the Internet. PPTP is documented in RFC 2637, and can be used for remote access and router-to-router VPN connections.

In Figure 15, the structure of a PPTP packet containing an IP datagram is illustrated. The figure shows how the payload of the encapsulated PPP frames is encrypted and/or compressed. In addition, for tunnel management, PPTP uses a TCP connection, and in order to encapsulate the PPP frames for tunneled data, PPTP uses a modified version of Generic Routing Encapsulation (GRE).

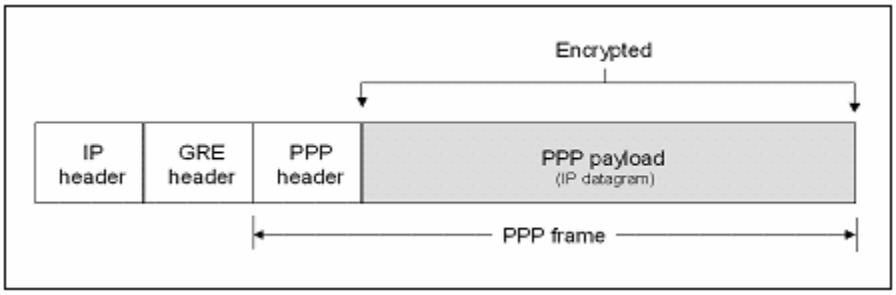

Figure 15. Structure of a PPTP Packet Containing an IP Datagram. (From Ref. [63].)

(2) Layer Two Tunneling Protocol (L2TP) - Layer Two Tunneling Protocol allows an organization to encrypt data that are of multi-protocol and then sent over any medium that supports point-to-point datagram delivery, such as IP, X.25, Frame Relay, or Asynchronous Transmission Mode. This protocol is combination of PPTP and Layer Forwarding, a technology proposed by Cisco Systems, Inc. [Ref. 63] L2TP is documented in RFC 2661, and can be used as a tunneling protocol over the Internet when it is configured to use IP as its datagram transport.

In Figure 16, the structure of the L2TP packet containing an IP datagram is illustrated. This figure shows the payloads of the encapsulated PPP frames

can be encrypted and/or compressed. For tunnel management, L2TP uses UDP and a series of L2TP messages, and for the tunneled data, L2TP uses UDP again to send L2TP encapsulated PPP frames.

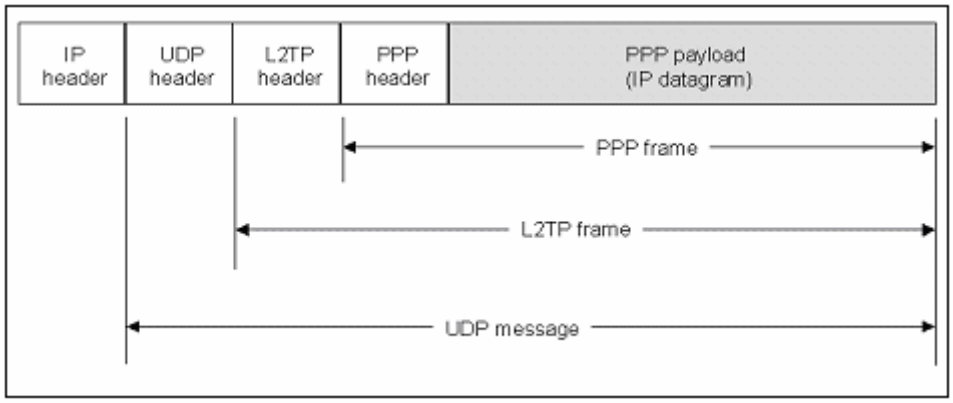

Figure 16. Structure of a L2TP Packet Containing an IP Datagram. (From Ref. [63].)

When encrypting L2TP traffic, Microsoft implements L2TP and uses IPSec Encapsulating Security Payload. This is documented in RFC 3193, and the combination of both L2TP and IPSec is known as L2TP/IPSec. Figure 17 shows the result of applying ESP to an IP packet that contains an L2TP message

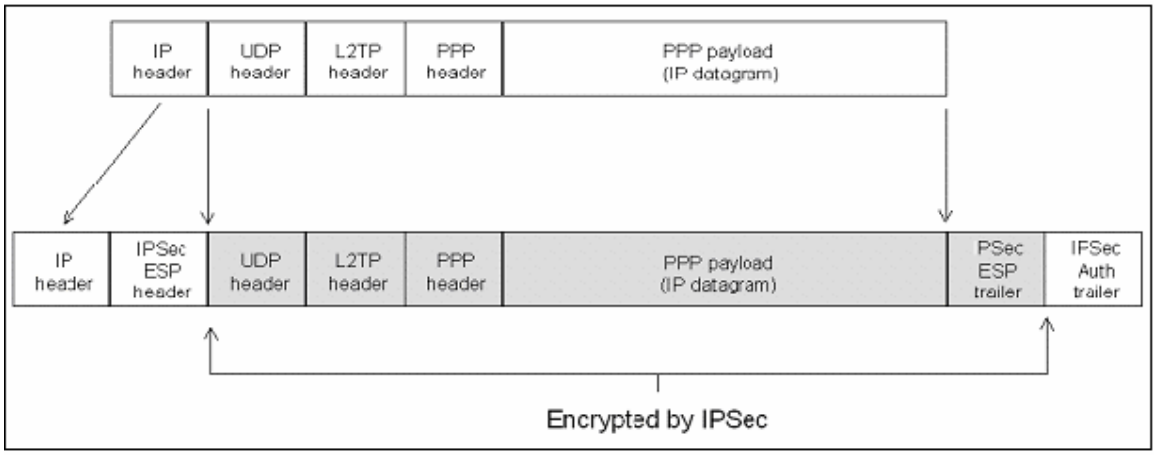

Figure 17. Encryption of L2TP Traffic with IPSec ESP. (From Ref. [63].)

Although both protocols use PPP, PPTP and L2TP are different. Both protocols, PPTP and L2TP, use PPP to provide the initial envelope for the data, and later append additional headers for transport via the Internet. Their differences are listed in the following:

- With PPTP, data encryption begins after the PPP connection process is completed. With L2TP/IPSec, data encryption begins before the PPP connection process by negotiating an IPSec security association.
- PPTP connections use Microsoft Point-to-Point Encryption, stream cipher that is based on the Rivest-Shamir-Aldeman (RSA) RC-4 encryption algorithm and uses 40, 56, or 128-bit encryption keys. Stream ciphers encrypt data as a bit stream. L2TP/IPSec connections use the Data Encryption Standard (DES), which is a block cipher that uses either a 56-bit key for DES or three 56-bit keys for 3-DES. Block ciphers encrypt data in discrete blocks, 64-bit blocks in the case of DES.
- PPTP connections require only user-level authentication through a PPP-based authentication protocol. L2TP/IPSec connections require the same user-level authentication and, in addition, computer-level authentication using computer certificates. [Ref.63]

The following list describes the advantages L2TP/IPSec has over PPTP in Windows Server 2003.

- IPSec ESP provides per-packet data origin authentication, data integrity, replay protection, and data confidentiality. In contrast, PPTP provides only per-packet data confidentiality.
- L2TP/IPSec connections provide stronger authentication by requiring both computer-level authentication through certificates and user-level authentication through a PPP authentication protocol.
- PPP packets exchanged during user-level authentication are never sent in an unencrypted form because the PPP connection process for L2TP/IPsec occurs after the IPSec security association is established. If intercepted, the PPP authentication exchange for some types of PPP authentication protocols can be used to perform offline dictionary attacks and determine user passwords. By encrypting the PPP authentication exchange, offline dictionary attacks are much more difficult, as the encrypted packets must first be successfully decrypted. [Ref. 63]

The next list provides the advantages of PPTP over L2TP/IPSec in Windows Server 2003.

- PPTP does not require a certificate infrastructure. L2TP/IPSec requires a certificate infrastructure for issuing computer certificates to the VPN server computer and all VPN client computers.
- PPTP clients can be placed behind a network address translator (NAT) if the NAT has an editor for PPTP traffic. L2TP/IPSec-based VPN clients or servers cannot be placed behind a NAT unless both the VPN client and the server support IPSec NAT traversal. [Ref. 63]

Using VPN on Windows Server 2003, Web and Standard editions, the systems administrator can create up to 100 PPTP ports and up to 100 L2TP ports. Windows Server 2003 Web edition can accept only one VPN connection at a time, while the Standard edition can accept up to 1,000 concurrent VPN connections via the ports. Therefore, if there were 1,000 clients connected, the system network would deny further connection attempts until the number of VPN connections went below 1,000. Lastly, Windows Server 2003, Enterprise and Datacenter editions, support unlimited concurrent users. [Ref. 63]

b. Network Bridge

The Network Bridge feature in Windows Server 2003, Standard and Enterprise editions, provides a means of connecting different local area network (LAN) segments and allows systems administrators to bridge connections between different computers and devices on the network. Basically, this feature eliminates the need to route and bridge hardware in a small office network that consists of multiple LAN segments. These multiple LAN segments will become a single IP subnet even if they are mixed with other network media types.

The Network Bridging process automatically configures and manages the address allocations, routes, and name resolution that are typically required in a network consisting of multiple LAN segments. Systems administrators must be cautious when using Network Bridging because setting up a Network Bridge between the public Internet connection and the private network connection will create an unprotected link between the organization's network and the Internet. This situation will leave the network vulnerable to external attacks, but this problem can be mitigated by either enabling ICF or ICS.

c. Internet Connection Sharing (ICS)

Internet Connection Sharing in Windows Server 2003 allows the systems administrator to enable Internet access for a small office network by using one common connection as the Internet gateway. The computer that is the ICS host will be the only computer that is directly connected to the Internet. This common connection allows multiple ICS clients to simultaneously use the link and benefit from Internet services as if the clients were directly connected to the Internet service providers. Another benefit of

ICS being enabled is how ICS enhances security because the ICS host computer is the only asset visible on the Internet. Through ICS, the addresses of ICS clients are hidden from the Internet, which renders ICS clients to be invisible to the Internet.

By enabling ICS on a computer that uses a dial-up or high speed Internet connection, the systems administrator can implement ICS, which will simplify the configuration process of small networks by providing local private network services like name resolution, Network Address Translation, and IP addressing. This simplification permits a systems administrator to share a single routable IP address and distribute unique IP addresses to all of the organization's other computers. When implementing ICS, it is recommended that the systems administrator only assign routable addresses to a small number of systems, and generally put the non-routable addresses to the majority of the organization's machines. [Ref. 1]

6. File and Print Services

File and Print Services is critical in any organization because it is imperative for users to have quick, guaranteed, and secure access to the organization's data. Windows Server 2003 has new features and improvements to its File and Print Services that can assist in facilitating the organization's required needs. The new features that will be discussed include the following: Distributed File System, Encrypting File System, Shadow Copy Restore, Shadow Copy Transport, Removable and Remote Storage, Fax Service, Services for Macintosh, Virtual Disk Service, and Volume Shadow Copy Service. With these new features in the File and Print Services, the systems administrator can mitigate the increasingly heavy burden that the organization is faced with as the organization's network expands with more users located on-site, in remote locations, or even at partner companies.

a. Distributed File System (DFS)

Distributed File System in Windows Server 2003 allows administrators to easily view, access, and manage files that are scattered across multiple file servers and other shared resources throughout an organization. By using DFS, systems administrators can make simple views of folders and files, a virtual organization called a "namespace," no matter where those files are physically residing in the network. Basically, a namespace creates a file path transparent from a user's perspective; this

simplified process is like a file system that provides a uniform name access to collections of sectors on a disk; DFS similarly is able to provide a uniform naming convention and mapping for a conglomerate of servers, shares, and files in the organization and its partners.

There are a number of enhanced features in the DFS in Windows Server 2003 that include the following:

- **Multiple Namespaces per DFS Server -** This feature allows a single Windows Server 2003 DFS server to host hundreds of DFS namespaces, supported by Enterprise and Datacenter editions only, which increases namespace without requiring additional servers.
- **Enhanced Multiple-Root DFS -** DFS has the capability to allow more than 16 root targets that can be scaled across in widely separated geographic locations. Factors such as size of the root target DFS namespace metadata will determine the number of root targets, which can range into the hundreds.
- **Integrated with Microsoft Active Directory Link Costing -** DFS can be used in an organization's existing Active Directory service, which will allow DFS to rank all available client-server connections by the site link cost defined in Active Directory. This process transparently allows users to access data from the nearest available file replica.
- **Dynamic Site Selection -** This feature allows Windows Server 2003 DFS root servers to dynamically detect when the DFS root servers or link targets change site. Systems administrators will be able to relocate servers to other parts of the organization's network much easier and ensures site selection remains predictable and efficient.
- **Enhanced Script-Based Management -** Windows Server 2003 enhanced command line tools allow for scripting creation, updates, and deletions of DFS namespaces, and have made it easier to manage DFS by using the scripts for monitoring and backing up DFS.
- **Improved Replication Management -** The DFS snap-in in Windows Server 2003 provides support for configurable replication topologies such as the ring, full mesh, hub-and-spoke, and custom. [Ref. 64]

In regards to the capability of a single server to host multiple DFS roots, this feature is a major improvement from Windows 2000, considering it could not have multiple DFS roots on a single server. This deficiency forced a large number of servers operating Windows 2000 to host multiple DFS roots, and fortunately this is not a restriction in Windows Server 2003. In addition, while Windows Server 2003 has the

capability to host multiple DFS roots, Windows 2000 clustered stand-alone DFS servers could host only one DFS root.

Lastly, Windows Server 2003 Standard edition can support only one DFS root, and the DFS is partially supported in Windows Server 2003 Web edition. In addition, Web edition is capable of accessing DFS files and acts as a node in the DFS tree, but it can only permit ten concurrent incoming Server Message Block connections.

b. Encrypting File System (EFS)

Encrypting File System in the Windows Server 2003 family is a transparent file encryption service that provides file confidentiality without providing any integrity or authentication protection. EFS complements other access controls and is able to provide an additional level of protection for an organization's data resources. In addition, this feature allows access to files when utilizing the optional data recovery capability, even if a user key is lost or destroyed. Another capability EFS offers is the capability to run as an integrated system service on all disks, including clustered disks, which makes the system easier to manage and difficult to attack.

In its implementation, EFS uses the standard X.509 certificates for all access credentials, and each protected file has an encryption, File Encryption Key (FEK), that is randomly generated by using a symmetric encryption algorithm. In processing encryption for a file, EFS wraps the FEK by encrypting it with the public keys from one or more EFS certificates. In order for a user to access an encrypted file, the user must have the private key that corresponds to one of the public keys used to wrap the FEK. Systems administrators must be careful with the private keys because any user that has access to one of the private keys may get access to a file by first decrypting the wrapped FEK with the private key and then decrypting the file with recovered FEK.

To reiterate, EFS creates a layer of security that transparently encrypts data on the physical disk without the need to have the end user interaction, which ensures the data to be much safer. This is especially important for data by personnel who are mobile users to prevent sensitive organizational data from being lost or stolen. Lastly, EFS allows for offline and Web folders to be encrypted and shared among multiple users.

c. Volume Shadow Copy Service (VSS)

Volume Shadow Copy Service is new to Windows Server 2003 and provides a built-in snapshot capability called "shadow copy." Shadow copies are created by VSS, which complements the systems administrator's tape backup archival system. The shadow copy used as a backup provides a high fidelity point-in-time copy that is created and restored easily. This section will discuss topics of VSS on Shadow Copies, Backups, Shadow Copy Restore, and Shadow Copy Transport.

(1) Shadow Copies - Shadow Copies in Windows Server 2003 mitigates the difficulties in recovering an individual's precious document that has been lost. This feature is included in Windows Server 2003 and as mentioned earlier, it helps in the recovery of old versions of user files when the files are accidentally deleted, corrupted, or edited. Systems administrators can benefit from implementing Shadow Copies by the following:

- Empower users to recover their own file quickly and easily.
- Eliminate the need to rebuild the file all over again.
- Decrease the IT department or help desk calls.
- Lower the cost and time spent in recovering lost data from backup tapes. [Ref. 65]

Systems administrators enabling Shadow Copies for the first time will be taking a snapshot of their organization's volume in the server. This snapshot will collect only the changes in the files and not the files themselves, which will save disk space. Also, the users will have the capability to access the shares on the server and return to the previous versions from the desktop.

When implementing Shadow Copies, systems administrators must take into consideration four key decision factors: source files, disk space, location copies, and schedule. For source files, Shadows Copies are taken from a complete volume and work best with user files from spreadsheets, documents, and presentations. This feature works with compressed or encrypted files, and it is able to retain whatever permissions previously set on the file. Systems administrators should not use Shadow Copies to provide access to previous version of application or e-mail databases. In addition, Shadow Copies work only on NTFS volumes.

When considering disk space, systems administrators enabling Shadow Copies on a volume should know that it uses 10 percent of disk space by default, but it can be changed by using the Settings tab [Ref.65]. If the 10 percent limit is reached, Shadow Copies will automatically overwrite the oldest version of the file. In addition, the amount of disk space Shadow Copies will use depends on the frequency of the users changing or altering files and not on how much data are actually being stored.

The location of copies will affect the performance of the disk. For example, when the snapshot starts, the burst disk IO will reduce the performance of the disk. But, using a separated volume on separated disks will provide improved performance and is recommended.

The scheduling of Shadow Copies is important and should meet the organization's mission needs. In Windows Server 2003, it creates, by default, Shadow Copies at 0700 to 1200 on Monday through Friday. The more frequent Shadow Copies are created, the more likely a desired version of the end user's file is acquired. But, the systems administrator must know that the maximum limit of Shadow Copies is 64 per volume. Systems administrators should be aware of users who are utilizing this feature because the more Shadow Copies that are created, the more disk space is used. The amount of Shadow Copies clients should be limited.

(2) Shadow Copy Backups - Shadow Copy Backup is a fast means of creating a point-in-line image for backups, which is usually in the order of seconds to a minute depending on the size of the data. This feature also will create an image without disrupting production servers. Using shadow copy technology, VVS has solved the problem of un-restorable backups due to the lack of coordination between the backup application and the end user applications, such as the databases. In this situation, there is an inconsistency in the data when applications are open and are being written to, while a backup is being processed. But, VSS solves this problem by coordinating with the backup service and the application to ensure that no writes to the disk are being made during the actual backup process. If a problem occurs during the backup process, VSS sends the requestor a notification that the shadow copy data are inconsistent and that the backup can be re-scheduled. This process improves the data integrity of backups. [Ref. 66]

(3) Shadow Copy Restore - Shadow Copy Restore provides point-in-time copies for network folders. This feature allows users easy access to previous versions of files through the Windows Explorer by right-clicking on a file or folder. Shadow copies are previous versions of files and by using shadow copies, any Windows Server 2003-based file server can transparently maintain a set of previous versions of all files on the file server. This feature can mitigate the human errors that causes over one third of all data loss. [Ref. 67]

(4) Shadow Copy Transport - Shadow Copy Transport utilizes the combination of hardware shadow copies and storage area network (SAN) mount or dismount capabilities. A shadow copy of storage volume is a point-in-time of the original volume, and Volume Shadow Copy Service (VSS) enables SAN products to create hardware shadow copies that can be virtually transported to another server for use. SAN products can mount and dismount hardware shadow copies from a production machine to a secondary machine no matter the data size. [Ref. 62]

d. Removable and Remote Storage

Removable and Remote Storage are features in Windows Server 2003 that utilizes one another to leverage other storage means. Remote Storage uses Removable Storage to access those infrequently used files and moves them from the hard disk onto the applicable media in a library to free up hard-disk space. This feature allows systems administrators to easily extend disk space on the organization's server computer without adding more hard disks. Remote Storage processing has criteria that can be specified by the systems administrator that will automatically copy eligible files on the local volumes to a library of magnetic tapes or magneto-optical disks. Then, the Remote Storage continues the process by monitoring the amount of space available on the local volumes and locates other infrequently used files to be moved.

When a user decides to access a file that has been untouched for a long period of time (several months), Remote Storage will locate the file on the magnetic tape in the library and places it back on the hard disk, which can be easily by the user. This process can be slow, but at least storage resources are made available for other mission critical tasks.

Removable Storage is used by Remote Storage because Removable Storage is able to easily track an organization's removable storage media such as tapes or optical discs and at the same time be able to manage the hardware libraries, such as changers and jukeboxes. Because removable optical discs and tapes are less expensive per megabyte than hard disks, Removable Storage and Remote Storage can decrease the spending in costly storage media. In addition, Remote Storage is not included in Windows, Standard and Web editions. [Ref. 62]

e. Fax Service

Fax Service in Windows Server 2003 allows systems administrators to share fax resources among multiple users and to manage network fax resources from a central location. With the Fax Service Manager in the Windows Server 2003 family, systems administrators can configure fax devices, and share fax printers that will permit network users to send and receive faxes through remote fax printer connections. This feature allows the organization to set up routing policies for incoming faxes, and specify outgoing fax rules to route outbound faxes to specific groups, based on dialing destinations. Fax Service gives systems administrators the means to set up archiving that will provide access to faxes previously sent or received. In addition, the Services can be configured for activity logging to track the use of fax resources.

Fax Service Manager in Windows Server 2003 is a Microsoft Management Console (MMC) snap-in. This MMC snap-in provides organizations a single location to manage the local fax devices, or manage and configure Fax on a remote computer. Some of Fax Service Manager's capabilities and ones already mentioned are listed below:

- Configure local fax devices attached to computers, and configure and manage Fax on a remote computer.
- Specify security settings to secure shared fax resources.
- Control the Fax Service to stop and start incoming and outgoing fax transmissions for all fax devices on a specific computer.
- Configure the Outbox to specify how outgoing faxes will be handled.
- Configure outgoing fax rules to direct outgoing faxes to certain fax devices or groups of devices.
- Enable delivery receipts to notify users when the faxes are sent.

- Enable routing methods for incoming faxes to direct incoming faxes to e-mail, a folder location, or to a printer.
- Configure archive settings for Sent Items, the archive folder for sent faxes, and for the Inbox, the archive folder for received faxes.
- Configure activity and event logging for fax activity. [Ref. 68]

To reiterate the Fax Service capabilities, it provides the fax user the means to send, receive, and manage faxes using a local fax device attached to the organization's computer or via remote fax printer connection. Fax Service Manager improves the managing of Fax Service, but, systems administrators must install Fax Service because it is not installed by default during Windows Setup. In addition, in order to remotely manage and configure devices and settings for Fax Service on another computer, the systems administrator or the fax administrator needs to have specific permissions in order to use the feature.

f. Services for Macintosh

Services for Macintosh allow the systems administrator to provide those users with Macintosh computers to access files stored on a computer running Windows Server 2003. This feature has three components: File Server for Macintosh, Print Server for Macintosh, AppleTalk protocol [Ref. 69]. File Server, called "MacFile," permits the systems administrator to designate a folder as a Macintosh-accessible volume that ensures Macintosh file names are legal NTFS names, and handles permissions appropriately. The file server can be through TCP/IP networks and AppleTalk networks.

Print Server, called "MacPrint," allows all network users to send print jobs to a spooler on the computer running Services for Macintosh and continue working without having to wait for the print jobs to finish. These Print services permit Macintosh clients to print to Windows NT or Windows 2000 based print shares through AppleTalk protocol.

AppleTalk protocol is the layer of AppleTalk Phase 2 protocols that delivers data to its destination on the network. With AppleTalk Phase 2 enhancements in routing and naming services of AppleTalk, the network will have improved traffic and better routing selection that can support more than 245 nodes and have multiple zones [Ref. 70].

g. Virtual Disk Service (VDS)

Virtual Disk Service gives systems administrator a means of managing multi-vendor storage devices by using a single Windows interface. VDS uses application programming interfaces (APIs) for storage hardware and for management of programs that manage storage hardware. This feature allows systems administrators to view multi-vendor storage devices and to configure the resources by using one unified interface. Before using VDS, each individual vendor's storage device had its own management API, and this resulted in numerous APIs in a mixed storage environment. In addition, VDS provides the systems administrator the flexibility to make a choice on how to access the standardized interface, whether graphically using a user interface or at the command prompt by using a command line interface.

7. Management Services

Management Services in Windows Server 2003 provides systems administrators the tools to manage a growing network infrastructure with a computing environment that has proliferated on desktops, laptops, and portable devices. With Windows Server 2003, the systems administrator can utilize the improvements in WSRM and Group Policy that can control resource allocations and a wide range of configuration issues such as user's desktops, settings, security, roaming profiles, Start menu options, and more. Group Policy and WSRM have been discussed in earlier sections, and, therefore, this section will focus on two features in the Management Services: IntelliMirror and Remote Operating System Installation.

a. IntelliMirror

IntelliMirror in Windows Server 2003 permits systems administrators to allow users consistent access to applications, application settings, and user data from any managed computer, even if the user is disconnected from the organization's network. The IntelliMirror technology is implemented as a set of other Windows technologies that allows administrators to create standard computing environments for groups of users and computers. By providing policy-based management of users, desktops, and servers, IntelliMirror can centrally define policies based on users' group memberships and location. In addition, machines operating on a Windows-based server and clients running

an operating system that Windows 2000 later can be configured to automatically meet a user's requirement every time the user logs on to the network.

The IntelliMirror has benefits when utilizing various features, in Windows Server 2003, that are both from the server and the client side that can be used together or separately, depending on the requirements of the computing environment. The following table highlights benefits to the users when IntelliMirror is deployed and identifies the different technologies that are enabled.

Table 8. IntelliMirror Benefits and Technologies. (From Ref. [71].)

Benefit	Description	Technologies
Consistent Environment	Users can work with a consistent computing environment from any computer, such as when their desktop or laptop computers are unavailable. Users' profiles are stored on a server so that the profiles are available from any machine. In cases where users are not assigned a specific computer, hardware and administration costs are reduced as well, because users can log on to any available IntelliMirror–managed computer and work in a familiar environment.	▪ Active Directory ▪ Group Policy ▪ Offline Folders ▪ Roaming User Profiles ▪ Redirected Folders ▪ Enhancements to the Windows Shell ▪ Group Policy Software Installation
Uninterrupted Access	Users can continue to work efficiently even when network connections are intermittent or even disconnected. Under these conditions, uninterrupted access to user and configuration data can be enabled. IntelliMirror eases the IT task of implementing centralized backup of user files while satisfying a need for these files to remain available on users' computers.	▪ Active Directory ▪ Group Policy ▪ Offline Folders ▪ Synchronization Manager ▪ Enhancements to the Windows Shell ▪ Redirected Folders ▪ Disk Quotas
Minimized Data Loss	IT organizations can enable centralized backup of user data and configuration files. Centralized backups ease the IT workload and satisfy users' need for files to remain available on their computers.	▪ Active Directory ▪ Group Policy ▪ Roaming User Profiles ▪ Redirected Folders ▪ Offline Folders
Minimized User Downtime	Administrators can enable automated installation and repair of applications, reducing support costs by using Windows Installer to repair application installations automatically.	▪ Active Directory ▪ Group Policy ▪ Windows Installer Service ▪ Add/Remove Programs in Control Panel ▪ Group Policy Software Installation

As mentioned earlier, IntelliMirror uses different Windows technologies to provide users the benefits listed in Table 8. Systems administrators should know that

IntelliMirror is not single entity; IntelliMirror is a marketing moniker for a group of Windows 2000, Windows XP, and Windows 2000 Desktop management features that can be easily implemented with group policies [Ref. 1].

b. Remote Operating System Installation

Remote Operating System (OS) Installation in Windows Server 2003 is a feature that uses Group Policy, Remote Installation Services (RIS), and Pre-Boot eXecution Environment (PXE) server hardware to re-image a server with a clean install of a Windows Server 2003 based environment. Windows 2000 and Windows XP desktops can be re-imaged as well. This feature allows systems administrators to use Remote OS Installation in conjunction with IntelliMirror to make the task of exchanging or bringing new computers into the network much easier. The process is made easier because Remote OS Installation establishes a full initial working set image directly to the computer hardware and IntelliMirror can restore policy-based settings for data, settings, and software use.

Remote Installation Services is a key feature used in Remote OS Installation. RIS allows the systems administrator to designate a server or set of servers as RIS servers. These RIS servers contain files necessary to remotely install Windows 2000, Windows XP, or Windows Server 2003 onto a computer from across the network. RIS can deliver an operating system to a computer in one of the following formats:

- **Simple I386 Based Installation -** Systems administrator goes to the intended computer to put install the OS and boot it with just one floppy. There is no hassle with DOS Client for networks or the like. But, once the installation has started up, the administrator must sit at the computer and answer all of the Setup's questions.
- **Scripted I386 Install -** This install is similar to the previous one, but has an added benefit of unattended installation. Again, the systems administrator goes to the intended computer, boot the floppy, and away it goes. These first two installs are called flat image format images.
- **Complete System Image with Minimal Setup Interaction -** In this install the systems administrator builds a prototypical machine running Windows 2000 Pro or Server, Windows XP, or Server 2003, complete with applications; and then, RIS is used to create an image of that machine on a RIS server. Then, boot the target computer with a RIS built floppy again, and RIS transfers the entire disk image with complete operating

> systems and applications to the target computer. This type of imaging is called a RIPrep image format image; unfortunately, it is not completely a hands-off process. [Ref. 1]

RIS is a great way to roll out operating systems to computers, but in order for the RIS server to process this task, the computers need to be built in a particular way that is required of the RIS server. RIS built computers, called "RIS clients," use PXE protocol to support the needed communication. Without PXE, the targeted computer is unable to get the RIS system image.

Lastly, RIS in Windows 2000 Server sends passwords in clear text over the network cable when the systems administrator first logs on. Although this happens only once, it is still bad in regards to security. But, this problem was resolved in Windows Server 2003 by revising clients to encrypt passwords before putting them on the wire. [Ref. 1]

8. .NET Application Services

.NET Application Services in Windows Server 2003 includes features such as .NET Framework, Internet Information Services 6.0, ASP.NET, and Enterprise UDDI (Universal Description, Discovery, and Integration) Services. This feature allows systems administrators to permit developers to extend existing code and write new applications and XML Web services. Considering the three forementioned features have been previously discussed, this section will discuss on the topic of Enterprise UDDI Services.

Enterprise UDDI Services is an industry specification for publishing and locating information about Web services. This feature permits organizations to run and operate their own UDDI directory for intranet or extranet use. Also, it helps organizations in organizing and cataloging Web services and other programmatic resources. By using the cataloging schemes such as geography, Quality of Service, or organizations in UDDI Services, an organization can create a structured and standardized process that will describe and discover services [Ref. 72].

Enterprise UDDI Services is not included in Windows Server 2003, Web edition; and, the Standard edition will support only stand alone installations of UDDI Services. On the other hand, the Enterprise edition and Datacenter edition support distributed

installation of UDDI Services. For a distributed installation, UDDI components are distributed across multiple servers. In contrast, a stand alone installation of UDDI Services has its components, both the UDDI Web server component and the UDDI database component, installed onto a single server.

9. Multimedia Services

Multimedia Services for Windows Server 2003 is featured in Windows Media Services. Windows Media Services is the server component of Windows Media 9 Series that is used to distribute digital media content over an organization's intranets and the Internet. Windows Media Services 9 Series, which has been completely redesigned and enhanced, is able to offer the traditional digital distribution services, such as file and Web services. Both Enterprise and Datacenter editions feature Windows Media Service, which also provides advanced streaming functionality, such as multicasting, wireless network support, Internet authentication, server plug-ins, and cache and proxy application programming interfaces [Ref. 62]. In Table 19 of Appendix A, it shows that the Standard edition partially supports Windows Media Service, while the Web edition has zero support for the feature.

C. CHAPTER SUMMARY

Windows Server 2003 has numerous new features and improvements that have taken advantage of old and new technological advances. The features highlighted in this chapter are important concepts in order to understand the operating system. Because there has been an increasing needs and advancements in IT technology, it is advantageous for the systems administrator to acquire the IT knowledge needed to effectively manage an organization's network. By knowing the features in Windows Server 2003 and how they function in a computing environment, systems administrators can plan for and manage an organizational network more effectively.

From deploying a Web server to securing a network for remote users, well-trained systems administrators of Windows Server 2003 operating systems will be more prepared in the deployment and management of an organization's IT infrastructure. Depending on the organization's mission needs and its IT infrastructure, Windows Server 2003 is robust and versatile in the new features and the various family editions it offers. This operating system is an effective tool to connect organizations to the wired world.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PROS AND CONS OF AN ORGANIZATION MIGRATING TO WINDOWS SERVER 2003

As with all new systems, Windows Server 2003 is not perfect. The changes made during the development of the operating system provide significant enhancements and improvements as discussed in the previous chapter. These enhancements and improvements are some of the major reasons to consider migrating to Windows Server 2003. However, the migration to Windows Server 2003 is not a task to be taken lightly whether the IT staff is upgrading from Windows 2000 or Windows NT. The process of upgrading from Windows 2000 Server is not as drastic of a migration process when compared with migrating from Windows NT. In regards to upgrading, this chapter will discuss some of the pros and cons of migrating to Windows Server 2003. Considering the numerous features encompassed in Windows Server 2003, the focus of discussion will be the following: scope, interoperability, cost, and training. For clarification, this chapter is intended to provide "good to know" information, and not procedures for a migration process.

A. SCOPE

The scope of migrating to Windows Server 2003 can vary depending on the size of the network, the number of servers it holds, and the number of users it serves. The migration process is a significant project that can adversely affect many personnel if not done properly. The scope of migrating to Windows Server 2003 can be overwhelming, especially if when migrating from Windows NT. Support for Microsoft's Windows NT Server will stop by the end of December 2004, prompting NT administrators to plan the migration process to the Windows 2000 Server or the Windows Server 2003 in order to maintain support in the future for their organization's network infrastructure. According to Gartner, an independent research and analysis company, the process of migrating can take as long as 12 to 18 months to complete for large companies with complex infrastructures. For smaller companies, with fewer servers, legacy systems, and users, the migration process can take as much as 3 to 9 months. [Ref. 73]

One overwhelming aspect of migrating to Windows Server 2003 is the migration of the Active Directory. The systems administrator of the organization will need to

conduct a lot of planning, testing, and documenting. While testing the migration plan or design, the systems administration can discover problems that can be resolved prior to the actual migration process. The tests and findings should be documented in order to recreate and/or prevent any problematic issues. The migration process is challenging. To help mitigate implementation issues during the process, well-trained IT staff can properly plan and test a proposed network before using the actual network in the production environment, which will provide a better understanding of the network system.

B. INTEROPERABILITY

Interoperability concerns with migrating to Windows Server 2003 arise in a mixed environment of Windows NT 4.0 and later versions of Windows that are rooted in changes to the printer driver architectural model. Windows NT 4.0 printer drivers, version 2 drivers, run in kernel mode, while Windows 2000 or later support user-mode drivers, and version 3 drivers, natively; and kernel-mode drivers solely for backward compatibility. Microsoft decided to support user-mode drivers because when a kernel-mode driver generates an error, it crashes the entire server. On the other hand, when a user-mode driver generates an error, the effects of the error are restricted to the process the driver runs in the spooler. It is much faster to restart the spooler versus rebooting the entire system, and other services provided by the server remain available. Essentially, selecting the proper driver will improve the system's interoperability. If the Windows CD utilized to migrate does not have the appropriate driver, the utility will prompt the systems administrator to obtain the most updated driver from the manufacturer. [Ref. 74]

If an organization uses zone files in the network infrastructure, when the systems administrator copies zone files to DNS servers running on Windows Server 2003, the administrator must manually verify the integrity of the zones. This verification is required to determine if the original third-party DNS server has caused interoperability problems on the network. If the server needs to be used, it is recommended that the server be taken offline or the systems administrator can use the server on the network to provide backup for the primary DNS server running Windows Server 2003.

In regards to dynamic integration with DHCP, it is only available on DNS servers running Windows 2000 and Windows Server 2003. In addition, DNS-DHCP integration is not supported by DHCP servers running under Windows NT Server 4.0 and earlier. [Ref. 75]

As mentioned in the previous chapter, Windows Server 2003 features a new SFU that allows developers to compile and natively run Unix programs and scripts. In addition, this feature includes and Interix subsystem that comes with the full set of Unix utilities and shells to support a single-rooted file system and a software development kit to port applications. According to Jason Zion, a software architecture at Microsoft Corporation,

> This architectural approach to host both environments (Windows with SFU running as a subsystem) allows applications to be constructed using Unix and Windows software components….New components can be built more easily using tools like Visual Studio, and the Microsoft enterprise software platform can be used to solve business problems without throwing away legacy Unix code. [Ref. 76]

Although some legacy software or hardware owned by an organization may have interoperability issues with Windows Server 2003, the organization can plan in the future to mitigate this problem by making purchases of new hardware and software that are certified for Microsoft products. Products with the logo "Designed for Windows" have been certified. By purchasing hardware and software with the logo, the systems administrator can have confidence that the product will work well with Microsoft Windows operating systems. Three more reasons to have the logo on future products are listed below:

- The product will be stable when running Windows.
- Related software or driver components can be easily installed or removed.
- Basic experiences with the product and the operating system will be the same or better after upgrading to future versions of Windows. [Ref. 77]

C. COST

Windows Server 2003 is not an inexpensive operating system. Other expenses to consider are new hardware requirements if the current system is not up to par in regards to systems specifications for the new operating system. Again, the organization may

need to upgrade workstation computers, networking equipment, and the list can go on. But depending on the organizations business needs, the Chief Information Officer of the organization must make the decision on which family edition to select. The tables in Appendix C list the price and licensing details of the different family editions, ranging from $399 to $3,999. For additional licenses, the cost ranges from $199 to $7,999. Reviewing the price ranges, the systems administrator must take into account the cost of the operating system and decide the best value.

In addition to the cost of the operating system, the training for IT personnel and their certifications is just as expensive or if not more than the operating system itself. The different Microsoft Certification courses offered are the following:

- Microsoft Certified Professional (MCP)
- Microsoft Certified Desktop Technician (MCDST)
- Microsoft Certified Systems Administrator (MSCA)
- Microsoft Certified Systems Engineer (MSCE)
- Microsoft Certified Database Administrator (MCDBA)
- Microsoft Certified Applications Developer (MCAD)
- Microsoft Certified Solutions Developer (MCSD)
- Microsoft Certified Trainer (MCT) [Ref. 78]

The functionality of IT infrastructure will determine what training requirements are needed. The list above shows just the key courses an organization should provide to IT personnel. The typical cost of a certification exam is $125. In addition, course cost will vary worldwide depending on the Microsoft Certified Partners for Learning Solutions programs that teach the courses.

D. TRAINING

Training for Windows Server 2003 may be costly, but the amount of money spent is worth it because the more training an IT staff acquires increase the IT department's ability to handle issues that may arise during the deployment of the operating system. In addition, experience of the IT staff is important, as well, which can be gained when conducting tests on mock networks that are used to observe and learning how the organization's network will function in the Windows Server 2003 environment. Training

is imperative for systems administrators and their IT staff to ensure the organization's network infrastructure can be maintained in a stable and available state.

If a systems administrator is not properly trained, the administrator may not be cognizant to some of the new features and settings that can be key information in keeping Windows Server 2003 operating effectively and efficiently. For example, a systems administrator who knows Windows 2000 needs to add an individual to a new group in the Windows Server 2003 Active Directory may think the person has full control in regards to permissions. But, the added person to the AD will receive read only permission. This feature of Windows Server 2003 improves the security of the network, but adds a little more work for the administrator to set the proper permissions required for the individual added to the AD.

Microsoft-certified training comes in wide range of courses from Microsoft Certified Professional to Microsoft Certified Trainer. Systems administrators must decide what training to provide to the IT staff that will best meet the organization's needs. These certification training courses should be given annually to keep IT personnel up to date on current information on Windows operating systems.

E. CONCLUSION

The migration process to Windows Server 2003 has a lot of pros and cons that can be discussed, but the key ones mentioned in this chapter are important for the organization to consider. The most obvious con to consider is the scope of the migration process. This process will depend on the size of the organization, but even with a small company, the systems administrator's task of migrating will be challenging and it can be overwhelming to plan and to decide on how to transform the organization's old system to Windows Server 2003.

Planning and testing are two key steps to a successful migration that will involve a lot of training, and in turn, it will require upfront funding for the training, software, and hardware requirements. The training acquired will prove beneficial because it will allow IT staff to make the right decisions in correcting the system to operate more properly with other applications or hardware. In addition, with an inappropriate plan and/or design for an IT infrastructure's transformation process can cause some network

downtime and delays of important services required from the network. But, with a lot of forethought and planning, the organization can save time and money in the long run.

V. CONCLUSION

As with any new product offering, Windows Server 2003 will be received with some skepticism. The new operating system had a tall order to fulfill considering Microsoft's claim of Windows Server 2003 being "secure by design, secure by default, and secure in deployment," Microsoft refers to this new initiative as "trustworthy computing." To achieve these goals, the Windows Server 2003 family editions were built around new IT technological advances and the core technology of the Windows 2000 Server. The end result provides many new features and enhancements, including IIS 6.0 to .NET Frameworks, designed to improve the computing environment of users.

As new viruses and hackers attack network systems on a daily basis, the security features and improvements in Windows Server 2003 are valuable tools to mitigate those security risks for a network system that is connected to the Internet. Remote access features like IIS 6.0 and IAS/RADIUS provide user's connectivity to the organization's IT infrastructure that is more secure and that is globally accessible. These requirements and other needs of the organization must be thoroughly evaluated by the Chief Information Officer (CIO) in order to maximize the benefits offered by Windows Server 2003.

In the author's opinion, most CIOs will discover the benefits of migrating to Windows Server 2003 to be worth the effort and investment. An organization's effort in planning and testing a well thought out migration process will pay significant dividends during the actual migration process. The sophistication and complexity of Windows Server 2003 also mandate that the IT staff be fully trained and kept aware of updates to the new the operating system before and after the migration process. This training is essential to maximize the benefits of Windows Server 2003 and to ensure the proper management and operation of the network.

In conclusion, the author believes DoD activities will be well served by the enhanced features and security improvements of Windows Server 2003. For most situations, the potential benefits will outweigh the costs of migrating from older operating systems.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: COMPARISON OF WINDOWS SERVER 2003 EDITIONS

Windows Server 2003 edition is a robust operating system with numerous functionalities and features. Its features are taken from Windows 2000 Server technology and other advances in IT technology to build a platform that can do more with less, in areas such as security, reliability, availability, and scalability. The features of the Windows Server 2003 family are compared in the following set of tables that are organized by function. Listed below is the legend:

- X - The feature is included.
- / - The feature is partially supported.
- - A blank space signifies that the feature is not included.

The tables listed are have distinguished feature highlights of Windows Server 2003 family into 11 functional areas.

- Hardware Specifications
- Directory Services
- Security Services
- Terminal Services
- Interoperability Tools
- Clustering Technologies
- Communications and Networking Services
- File and Print Services
- Management Services
- .NET Application Services
- Multimedia Services

Table 9. Hardware Specifications. (After Ref. [79].)

Feature	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
64- Bit Support for Intel Itanium		X	X	
Hot Add Memory		X	X	
Non-Uniform Memory Access		X	X	
Datacenter Program			X	
2 GB RAM Maximum				X
4 GB RAM Maximum	X			
32 GB RAM Maximum		X		
64 GB RAM Maximum		/	X	
512 GB RAM Maximum			/	
2-Way Symmetric Multi-processor	X	X		X
4-Way Symmetric Multi-processor	X	X		
8-Way Symmetric Multi-processor		X	X	
32-Way Symmetric Multi-processor			X	
264Way Symmetric Multi-processor			X	

Table 10. Directory Services. (After Ref. [79].)

Feature	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
Active Directory	X	X	X	/
Meta-Directory Services (MMS) Support		X	X	

Table 11. Security Services. (After Ref. [79].)

Feature	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
Internet Connection Firewall	X	X		
Public Key Infrastructure, Certificate Service, and Smart Cards	/	X	X	/

Table 12. Terminal Services. (After Ref. [79].)

Feature	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
Remote Desktop for Administration	X	X	X	X
Terminal Server	X	X	X	
Terminal Server Session Directory		X	X	

Table 13. Interoperability Tools. (After Ref. [79].)

Feature	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
Services for UNIX	X	X	X	X

Table 14. Clustering Technologies. (After Ref. [79].)

Feature	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
Network Load Balancing	X	X	X	X
Cluster Service		X	X	

Table 15. Communications and Networking Services. (After Ref. [79].)

Feature	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
Virtual Private Network (VPN) Support	X	X	X	/
Internet Authentication Service (IAS)	X	X	X	
Network Bridge	X	X		
Internet Connection Sharing	X	X		
IPv6	X	X	X	X

Table 16. File and Print Services. (After Ref. [79].)

Feature	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
Distribute File System (DFS)	X	X	X	/
Encrypting File System	X	X	X	X
Shadow Copies of Shared Folders	X	X	X	X
Shadow Copy Transport		X	X	
Removable Storage	X	X	X	X
Remote Storage		X	X	
Fax Service	X	X	X	
Services for Macintosh	X	X	X	
Service for UNIX	X	X	X	X
Virtual Disk Service (VDS)	X	X	X	X
Volume Shadow Copy Service (VSS)	X	X	X	X

Table 17. Management Services. (After Ref. [79].)

Feature	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
IntelliMirror	X	X	X	/
Group Policy Results	X	X	X	/
Windows Management Instrumentation (WMI) Command Line	X	X	X	X
Remote OS Installation	X	X	X	X
Remoter Installation Services (RIS)	X	X	X	
Windows System Resource Manager (WSRM)		X	X	

Table 18. .NET Application Services. (After Ref. [79].)

Feature	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
.NET Framework	X	X	X	X
Internet Information Services (IIS) 6.0	X	X	X	X
ASP.NET	X	X	X	X
Enterprise UDDI Services	X	X	X	

Table 19. Multimedia Services. (After Ref. [79].)

Feature	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
Windows Media Services	/	X	X	

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B: LIST OF SCRIPTS TO ADMINISTER A GROUP POLICY ENVIRONMENT

Group Policy-related tasks are directly administered by utilizing scripts that are mostly written in VBScript. The scripts are installed in the *%programfiles%\gpmc\scripts* directory, and all of the scripts are intended for command line operation. The table below shows a list of scripts that are provided to do the associated types of Group Policy administrative tasks.

Table 20. List of Scripts Providing Associated Types of Group Policy Administrative Tasks. (From Ref. [58].)

Administrative Task	Script Name	Description
Back up a GPO	BackupGPO.wsf	Backs up all GPOs in a domain to the specified backup directory.
Back up all GPOs in a domain	BackupAllGPOs.wsf	Given a GPO name or a GUID, backs up the GPO to a specified backup directory.
Create a GPO with default options	CreateGPO.wsf	Creates a GPO with the specified name, in the current domain, using the default options.
Create a migration table	CreateMigrationTable.wsf	Populates the entries of a migration table with security principals and UNC paths that are referenced in a GPO or backup.
Copy a GPO	CopyGPO.wsf	Creates a new GPO and copies the settings from the source GPO into the new destination GPO, given a source GPO name or GUID and a new destination GPO name.
Create a policy environment using an XML representation	CreateEnvironmentFromXML.wsf	Reads an XML file that specifies a policy environment; for example, OUs, GPOs, links, and security groups. The script can either create the environment in a domain by creating the objects, or delete the environment by deleting objects specified in the XML file.
Create an XML representation of a policy environment	CreateXMLFromEnvironment.wsf	Reads an existing policy environment and creates an XML file representing that environment. The XML file captures information about OUs, GPOs, and GPO links, and security on GPOs. You can use this script in conjunction with the CreateEnvironmentFromXML.wsf script to create a replica of domain for staging purposes.
Delete a GPO	DeleteGPO.wsf	Deletes the specified GPO when given a GPO name or GUID. By default the script deletes links to that GPO within the same domain.
Grant Permissions for all GPOs in a Domain	GrantPermissionOnAllGPOs.wsf	Grants a user or group the specified level of permission for all GPOs in the specified domain.

Generate a report for a GPO	GetReportsForGPO.wsf	Creates an HTML and XML report for a given GPO at a given location in the file system.
Generate a report for all GPOs in the domain	GetReportsForAllGPOs.wsf	Creates HTML and XML reports for all GPOs in the domain, at a given location in the file system.
Import settings into a GPO	ImportGPO.wsf	Imports the settings from the specified backup to the existing destination GPO in the domain
Import multiple GPOs into a domain	ImportAllGPOs.wsf	Creates a new GPO and imports settings into that GPO for each backed-up GPO stored at a specific file system location.
Restore a GPO	RestoreGPO.wsf	Restores a backed-up GPO.
Restore all GPOs	RestoreAllGPOs.wsf	Restores all GPOs that are stored at a given file system location
Grant permissions for GPOs linked to a domain, OU, or site	SetGPOSecurityBySOM.wsf	Grants a user or group the specified permission type for all GPOs that are linked to a specified domain, OU, or site. You can specify **Read, Apply, Edit, FullEdit,** or **None** for the permission type.
Set GPO permissions	SetGPOPermissions.wsf	Sets the permission level for a security principal on a given GPO. You can specify **Read, Apply, Edit, FullEdit,** or **None** for the permission type.
Set permissions to create GPOs	SetGPOCreationPermissions.wsf	Grants or removes the ability to create GPOs in a domain for a given security principal.
Set policy-related permissions on a given site, domain, or OU	SetSOMPermissions.wsf	Sets policy-related permissions on a given scope of management (SOM). A SOM is any site, domain, or OU.
List all GPOs in a domain	ListAllGPOs.wsf	Prints all GPOs in the specified domain.
List disabled GPOs	FindDisabledGPOs.wsf	Prints all GPOs in the specified domain that are disabled or partially disabled.
List GPO information	DumpGPOInfo.wsf	Prints the information for a specific GPO, including creation time, modification time, owner, status, version number, links, security groups that filter the GPO, and security groups that have full control, edit, read, or custom permissions.
List scope of management information	DumpSOMInfo.wsf	Prints all information for a specific Scope of Management (SOM), including GPO links and policy related permissions on the SOM. A SOM is any site, domain, or OU.
List GPO by policy extension	FindGPOsByPolicyExtension.wsf	Prints all GPOs in the specified domain for which a specific policy extension is configured; for example, find all GPOs that contain the Software Installation or Folder Redirection policy settings.
List GPOs by security group	FindGPOsBySecurityGroup.wsf	Prints all GPOs that for which a given security principal has the specified permission on that GPO. You can specify **Read, Apply, Edit,** or **Fulledit** for the permission type.
List GPOs with duplicate names	FindDuplicateNamedGPOs.wsf	Prints all GPOs in the specified domain that have duplicate names.
List GPOs without Apply	GPOsWithNoSecurityFiltering.wsf	Prints all GPOs in the specified domain that do not

permission		apply to anyone because **Apply** permission is not set on the GPO.
List GPOs Orphaned in SYSVOL	FindOrphanedGPOsInSYSVOL.wsf	Finds and prints all GPOs in SYSVOL with no corresponding component in Active Directory.
List domains and OUs with external GPO links	FindSOMsWithExternalGPOLinks.wsf	Prints all domains and OUs in the specified domain that link to a GPO in a different domain.
List unlinked GPOs in a domain	FindUnlinkedGPOs.wsf	Prints all GPOs in the specified domain that have no links. Links outside the domain, including site links, are not checked.
Print the scope of management policy tree	ListSOMPolicyTree.wsf	Prints all SOMs in the specified domain with the list of GPOs that are linked to the domain and each OU.
List GPO backups in a given file system location	QueryBackupLocation.wsf	Prints information about all backed up GPOs at the file system location specified by the user.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C: WINDOWS SERVER 2003 PRICING

The Windows Server 2003 licensing model consists of a Server operating system license and incremental Client Access Licenses (CALs). The tables below shows the cost of Microsoft offers and licenses in regards to pricing and licensing.

** These products are only available through qualified OEMs.

*** These products are only available through volume licensing programs.

Table 21. Microsoft Windows Product Offering Pricing. (After Ref. [80].)

Product Offering	U.S. Price	Description
Windows Server 2003, Standard Edition	$999	Standard Server product plus 5 CALs (User or Device, chosen after purchase).
Windows Server 2003, Standard Edition	$1,199	Standard Server product plus 10 CALs (User or Device, chosen after purchase).
Windows Server 2003, Enterprise Edition, 32-bit version	$3,999	Enterprise Server product plus 25 CALs (User or Device, chosen after purchase).
Windows Server 2003, Enterprise Edition, 64-bit version	Same as 32-bit version	Enterprise Server product, but not available through retail channel, therefore number and type of CALs are chosen separately. Can be acquired through volume licensing agreement or OEM.
Windows Server 2003, Datacenter Edition	**	Available in 32-bit and 64-bit versions. Includes 5 CALs (User or Device, chosen after purchase).
Windows Server 2003, Web Edition	$399	Web Server product, no CALs required. Windows Server 2003, Web Edition, is not available in all channels. Open NL estimated price is $399. Contact your local System Builder, OEM, or reseller for actual prices or for more information on how to purchase.

Table 22. Client Access Licenses Pricing. (After Ref. [80].)

Client Access Licenses	U.S. Price	Description
Windows Server 2003, Client Access License 5-pack	$199	5 additional Windows Server 2003 CALs (User or Device, chosen at time of purchase)
Windows Server 2003, Client Access License 20-pack	$799	20 additional Windows Server 2003 CALs (User or Device, chosen at time of purchase)
Windows Server 2003, TS Client Access License 5-pack	$749	5 additional Windows Server 2003 Terminal Server (TS) CALs (User or Device, chosen at time of purchase)
Windows Server 2003, TS Client Access License 20-pack	$2,979	20 additional Windows Server 2003 TS CALs (User or Device, chosen at time of purchase)

Table 23. Connectors Pricing. (After Ref. [80].)

Connectors	U.S. Price	Description
Windows Server 2003, External Connector License	$1,999***	Optional additional server license for External Users accessing Windows Server 2003 software
Windows Server 2003, Terminal Server External Connector License	$7,999***	Optional additional server license for External Users accessing Windows Server 2003 Terminal Server

LIST OF REFERENCES

1. Minasi, Mark, and others, *Mastering Windows Server 2003*, 4th ed., Sybex, 2003.

2. Smith, Randal Franklin, "Unwrapping Win2003." [http://infosecuritymag.techtarget.com/2003/apr/cover.shtml]. September 2004.

3. Microsoft Corporation, "The Journey to Trustworthy Computing: Microsoft Execs Report First-Year Progress." [http://www.microsoft.com/presspass/features/2003/jan03/01-15twcanniversary.asp]. September 2004.

4. Burns, Christine and Shaw, Keith, "Operating Systems." [htpp://www.nwfusion.com/best/2004/0223os.html]. September 2004.

5. Microsoft Corporation, "Overview of Windows Server 2003, Standard Edition." [http://www.microsoft.com/windowsserver2003/evaluation/overview/standard.mspx]. September 2004.

6. Microsoft Corporation, "Overview of Windows Server 2003, Enterprise Edition." [http://www.microsoft.com/windowsserver2003/evaluation/overview/enterprise.mspx]. September 2004.

7. Microsoft Corporation, "Overview of Windows Server 2003, Datacenter Edition." [http://www.microsoft.com/windowsserver2003/evaluation/overview/datacenter.mspx]. September 2004.

8. Microsoft Corporation, "Overview of Windows Server 2003, Web Edition." [http://www.microsoft.com/windowsserver2003/evaluation/overview/web.mspx]. September 2004.

9. Microsoft Corporation, "Product Overview for Windows Small Business Server 2003." [http://www.microsoft.com/WindowsServer2003/sbs/overview.mspx]. September 2004.

10. Silwa, Carol, "Sidebar: New Security-Related Features in Windows Server 2003." [http://www.computerworld.com/securitytopics/security/story/0,10801,87822,00.html]. September 2004.

11. Microsoft Corporation, "Windows Server 2003 Security." [http://download.microsoft.com/download/9/a/f/9af7659a-f2f8-4a84-90f7-3c12b400066b/SecInnovation.doc]. September 2004.

12. Riley, Steve, “Ask Us About…Security October 30, 2001.” [http://www.microsoft.com/technet/archive/community/columns/security/askus/aus1001.mspx]. September 2004.

13. Microsoft Corporation, “What is IAS?” [http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/Default.asp?url=/resources/documentation/windowsServ/2003/all/techref/en-us/w2k3tr_ias_what.asp]. September 2004.

14. Microsoft Corporation, “Authentication Using Windows Technology: The Windows Platform Provides a Full RADIUS Solution for Centrally Controlling Who Can Connect to Your Network, and Their Level of Access.” [http://download.microsoft.com/download/5/4/c/54c7fec4-5deb-4aa6-9942-d2af0fb9b589/IASOverview.pdf]. September 2004.

15. Davies, Joseph, “RADIUS Protocol Security and Best Practices.” [http://download.microsoft.com/download/2/1/b/21b2c25d-31bd-4ea9-a231-caab6d02b855/RADIUS_Sec.doc]. September 2004.

16. Microsoft Corporation, “What’s New in Windows Server 2003 Security.” [http://www.microsoft.com/WindowsServer2003/evaluation/overview/technologies/security.mspx]. September 2004.

17. Mullins, Michael, “Get Acquainted with Windows Server 2003 Security Features.” [http://techrepublic.com.com/5100-6268-5074200.html]. September 2004.

18. Microsoft Corporation, “The Advantages of Protected Extensible Authentication Protocol (PEAP): A Standard Approach to User Authentication for IEEE 802.11 Wireless Network Access.”. [http://download.microsoft.com/download/4/4/7/447404a7-c373-4bf4-9c77-daee54b1f6fc/PEAP.doc]. September 2004.

19. Microsoft Corporation, “Securing Wireless LANs with PEAP and Passwords, Introduction: Choosing a Strategy for Wireless LAN Security.” [http://www.microsoft.com/technet/security/guidance/peap_int.mspx]. September 2004.

20. Microsoft, “Using Software Restriction Policies to Protect Against Unauthorized Software.” [http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx?pf=true#XSLTsection135121120120]. September 2004.

21. Microsoft Corporation, “The Cable Guru – December 2002.” [http://www.microsoft.com/technet/community/columns/cableguy/cg1202.mspx?pf=true]. September 2004.

22. Smith, Randal F., “Locking Down IIS: Microsoft Makes Good on Its Promise To Make Win2003’s Internal Web Server Secure by Default.” [http://infosecuritymag.techtarget.com/2003/apr/lockdown.shtml]. September 2004.

23. Microsoft Corporation, “Security Enhancements in Internet Information Services 6.0.” [http://www.microsoft.com/WindowsServer2003/techinfo/overview/iisenhance.mspx]. September 2004.

24. Microsoft Corporation, “Internet Information Services (IIS) 6.0 Security Overview.” [http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/enus/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/iis_security.asp]. September 2004.

25. Microsoft Corporation, “About Security.” [http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/enus/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sec_aboutsecurity.asp]. September 2004.

26. Thangarathinam, Thiru, “IIS and ASP.NET: The Application Pool.” [www.developer.com/net/asp/article.php/2245511]. September 2004.

27. Policht, Marcin, “Windows Server 2003: Hardware-Based Security.” [http://www.enterpriseitplanet.com/security/features/article.php/11321_3353591_2]. September 2004.

28. Microsoft Corporation, “FIPS 140 Evaluation.” [http://www.microsoft.com/technet/security/topics/issues/fipseval.mspx]. September 2004.

29. Microsoft Corporation, “Advanced Digest Authentication.” [http://www.microsoft.com/resources/documentation/WindowsServ/2003/datacenter/proddocs/enus/Default.asp?url=/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-us/sec_auth_advdigestauth.asp]. September 2004.

30. Microsoft Corporation, “Windows Data Protection.” [http://msdn.microsoft.com/library/default.asp?url=/library/enus/dnsecure/html/windataprotection-dpapi.asp]. September 2004.

31. Policht, Marcin, “Exploring Windows 2003 Security: Certificate Services.” [http://www.serverwatch.com/tutorials/article.php/3084941]. September 2004.

32. Microsoft Corporation, “INFO: Digital Signature Support in Windows Installer 2.0.” [http://support.microsoft.com/default.aspx?scid=kb;en-us;304111]. September 2004.

33. Microsoft Corporation, “New Features in Certificate Services.” [http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/enus/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_CS_whatsnew.asp]. September 2004.

34. Odhner, Nils, “Secure and Manage Windows Server 2003.” [http://www.ftponline.com/wss/2003_TE/magazine/columns/security/default_pf.aspx]. September 2004.

35. Microsoft Corporation, “Deploying & Supporting Windows Server 2003.” [http://www.microsoft.com/technet/itsolutions/msit/deploy/win2003.mspx]. September 2004.

36. Intel Corporation, “Intel Architecture Running Microsoft Windows Server 2003.’ [http://www.intel.com/ebusiness/pdf/prod/server/server2003/ar031405.pdf]. September 2004.

37. [Ref. 6]Microsoft Corporation, “Introducing the Windows Server 2003 Family.” [http://www.microsoft.com/WindowsServer2003/evaluation/overview/family.mspx]. September 2004.

38. Microsoft Corporation, “System Requirements.” [http://www.microsoft.com/windowsserver2003/evaluation/sysreqs/default.mspx]. September 2004.

39. Microsoft Corporation, “Windows Server 2003 Clustering.” [http://www.microsoft.com/WindowsServer2003/techinfo/overview/bdmtdm/default.mspx]. September 2004.

40. Pfeil, Ken, “Authentication Vulnerability in Microsoft Meta-Directory Services 2.2.” [http://download.microsoft.com/download/mms22/Patch/Q317138/NT5/EN-US/Q317138.EXE]. September 2004.

41. Microsoft Corporation, “Hot-Add Memory Support in Windows Server 2003.” [http://www.microsoft.com/whdc/system/pnppwr/hotadd/hotaddmem.mspx]. September 2004.

42. Microsoft Corporation, “Application Software Considerations for NUMA-Based Systems.” [http://www.microsoft.com/whdc/system/platform/server/datacenter/numa_isv.mspx?pf=true]. September 2004.

43. Microsoft Corporation, “Session Directory and Load Balancing Using Terminal Server.” [http://download.microsoft.com/download/8/6/2/8624174c-8587-4a37-8722-00139613a5bc/SessionDirectory.doc]. September 2004.

44. Microsoft Corporation, “Overview of the Session Directory Technology in Terminal Services.” [http://support.microsoft.com/default.aspx?scid=kb;en-us;301926]. September 2004.

45. Microsoft Corporation, “Windows System Resource Manger—Fast Facts.” [http://www.microsoft.com/WindowsServer2003/techinfo/overview/wsrmfastfacts.mspx?pf=true]. September 2004.

46. Microsoft Corporation, “Overview of Windows Server 2003, Datacenter Edition.” [http://www.microsoft.com/WindowsServer2003/evaluation/overview/datacenter.mspx#XSLTsection123121120120]. September 2004.

47. Microsoft Corporation, “Physical Address Extension – PAE Memory and Windows.” [http://www.microsoft.com/whdc/system/platform/server/PAE/PAEdrv.mspx]. September 2004.

48. Microsoft Corporation, “Microsoft Windows-Based Servers and Intel Hyper-Threading Technology.” [http://www.microsoft.com/Windows2000/server/evaluation/performance/reports/hyperthread.asp]. September 2004.

49. Microsoft Corporation, “Introduction to System Area Networks.” [http://msdn.microsoft.com/library/default.asp?url=/library/enus/network/hh/network/san_4e948c13-38c8-4c68-8415-5aff51bc24bf.xml.asp]. September 2004.

50. Microsoft Corporation, “What’s New in Internet Information Services 6.0.” [http://www.microsoft.com/WindowsServer2003/evaluation/overview/technologies/iis.mspx]. September 2004.

51. Microsoft Corporation, “Microsoft Knowledge Base Article – 305140: INFO: ASP.NET Roadmap.” [http://support.microsoft.com/default.aspx?scid=kb;en-us;305140]. September 2004.

52. Microsoft Corporation, “What’s New in the .NET Framework 1.1.” [http://msdn.microsoft.com/netframework/technologyinfo/overview/whatsnew/default.aspx]. September 2004.

53. Microsoft Corporation, “Introduction to IP Version 6.” [http://www.microsoft.com/WindowsServer2003/technologies/ipv6/introipv6.mspx]. September 2004.

54. Microsoft Corporation, “What is Domain Rename?” [http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/enus/Default.asp?url=/resources/documentation/WindowsServ/2003/all/techref/en-us/w2k3tr_domrn_what.asp]. September 2004.

55. Microsoft Corporation, “Understanding How Domain Rename Works.” [http://download.microsoft.com/download/9/6/5/965e6899-e086-4b3e-8ed6-516ea07ea225/Domain-Rename-Intro.doc]. September 2004.

56. Microsoft Corporation, “How the Active Directory Schema Works.” [http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/enus/Default.asp?url=/resources/documentation/WindowsServ/2003/all/techref/en-us/w2k3tr_schem_how.asp]. September 2004.

57. Microsoft Corporation, “Active Directory Application Mode Technical Reference (DRAFT).” [http://www.microsoft.com/downloads/details.aspx?familyid=96c660f7-d932-4f59-852c-2844b343f3e0&displaylang=en]. September 2004.

58. Microsoft Corporation, “Administering Group Policy with Group Policy Management Console.” [http://download.microsoft.com/download/a/9/c/a9c0f2b8-4803-4d63-8c32-3040d76aa98d/GPMC_Administering.doc]. September 2004.

59. Microsoft Corporation, “Remote Administration of Windows Servers Using Remote Desktop for Administration.” [http://download.microsoft.com/download/9/6/3/9633a6e7-9910-45b6-add3-d15483f68d24/tsremoteadmin.doc]. September 2004.

60. Microsoft Corporation, “Technical Overview of Terminal Services.” [http://download.microsoft.com/download/2/8/1/281f4d94-ee89-4b21-9f9e-9accef44a743/TerminalServerOverview.doc]. September 2004.

61. Microsoft Corporation, “Services for UNIX: New Features Guide.” [http://download.microsoft.com/download/6/d/8/6d8210f1-49b9-457e-816b-860242f2d5ef/sfu35new.doc]. September 2004.

62. Microsoft Corporation, “Windows Server 2003 Feature Highlights.” [http://www.microsoft.com/WindowsServer2003/evaluation/features/highlights.mspx]. September 2004.

63. Microsoft Corporation, “Virtual Private Networking with Windows Server 2003: Overview.” [http://download.microsoft.com/download/0/e/3/0e354109-5a05-48f2-a557-8c49f5230d8f/vpnoverview.doc]. September 2004.

64. Microsoft Corporation, “Simplifying Infrastructure Complexity with the Windows Distributed File System.” [http://download.microsoft.com/download/b/4/1/b4162ea1-c6d0-45a2-96f2-2b925e160204/dfs.doc]. September 2004.

65. Paz, Erez, “Professor Windows – April 2004: Love at First Snapshot (Shadow Copies on Windows Server 2003).” Microsoft Technet. [http://www.microsoft.com/technet/community/columns/profwin/pw0404.mspx#XSLTsection124121120120]. September 2004.

66. Microsoft Corporation, “Storage Management Using Windows Server 2003 and Windows Storage Server 2003 Virtual Disk Service and Volume Shadow Copy Service.” [http://download.microsoft.com/download/5/0/f/50f52e09-a217-4db7-ade1-5f3c42b4d99b/StorageMgtUsingVDSandVSS.doc]. September 2004.

67. Microsoft Corporation, “Technical Overview of File Services.” [http://download.microsoft.com/download/1/1/3/113f6ce1-a87e-4740-a30d-1dcb72a39a72/FileOverview.doc]. September 2004.

68. Microsoft Corporation, “Fax Service Manager Overview.” [http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/fxsclnt/FaxC_C_FaxServiceManager.asp]. September 2004.

69. Microsoft Corporation, “Understanding Services for Macintosh.” [http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/enus/Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/sfmunderstandtopnode.asp]. September 2004.

70. Microsoft Corporation, “Phase 2 AppleTalk Networks.” [http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/enus/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_SFMplanning_6.asp]. September 2004.

71. Microsoft Corporation, “Introduction to Group Policy in Windows Server 2003.” [http://download.microsoft.com/download/0/0/4/0044470e-5f3a-4569-9255-91f932e4da3b/gpintro.doc]. September 2004.

72. Microsoft Corporation, “What’s New in Enterprise UDDI Services.” [http://www.microsoft.com/WindowsServer2003/evaluation/overview/dotnet/uddi.mspx]. September 2004.

73. Cohen, Beth, and German, Hallett, “Practically Painless NT to Windows Server 2003 Migration: Preparation and Planning.” [http://networking.earthweb.com/netsysm/article.php/3071741]. September 2004.

74. Microsoft Corporation, “Print Server Upgrade, Migration, and Interoperability.” [http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/technologies/fileprint/psumio.mspx]. September 2004.

75. Microsoft Corporation, “Interoperability Issues.” [http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_DNS_imp_Interoperability.asp]. September 2004.

76. Ramesh, Ravind, “Microsoft Grants ‘Interoperability’ Wish.” [http://startechcentral.com/tech/story.asp?file=/2004/9/1/technology/8787594&sec=technology]. September 2004.

77. Microsoft Corporation, “Why Get the “Designed for Windows” Logo?” [http://www.microsoft.com/whdc/winlogo/benefits/default.mspx]. September 2004.

78. Microsoft Corporation, “Microsoft Certifications: Overview.” [http://www.microsoft.com/learning/mcp/default.asp]. September 2004.

79. Microsoft Corporation, “Compare the Editions of Windows Server 2003.” [http://www.microsoft.com/WindowsServer2003/evaluation/features/compareeditions.mspx]. September 2004.

80. Microsoft Corporation, “Windows Server 2003 Pricing.” [http://www.microsoft.com/WindowsServer2003/howtobuy/licensing/pricing.mspx?pf=true]. September 2004.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California